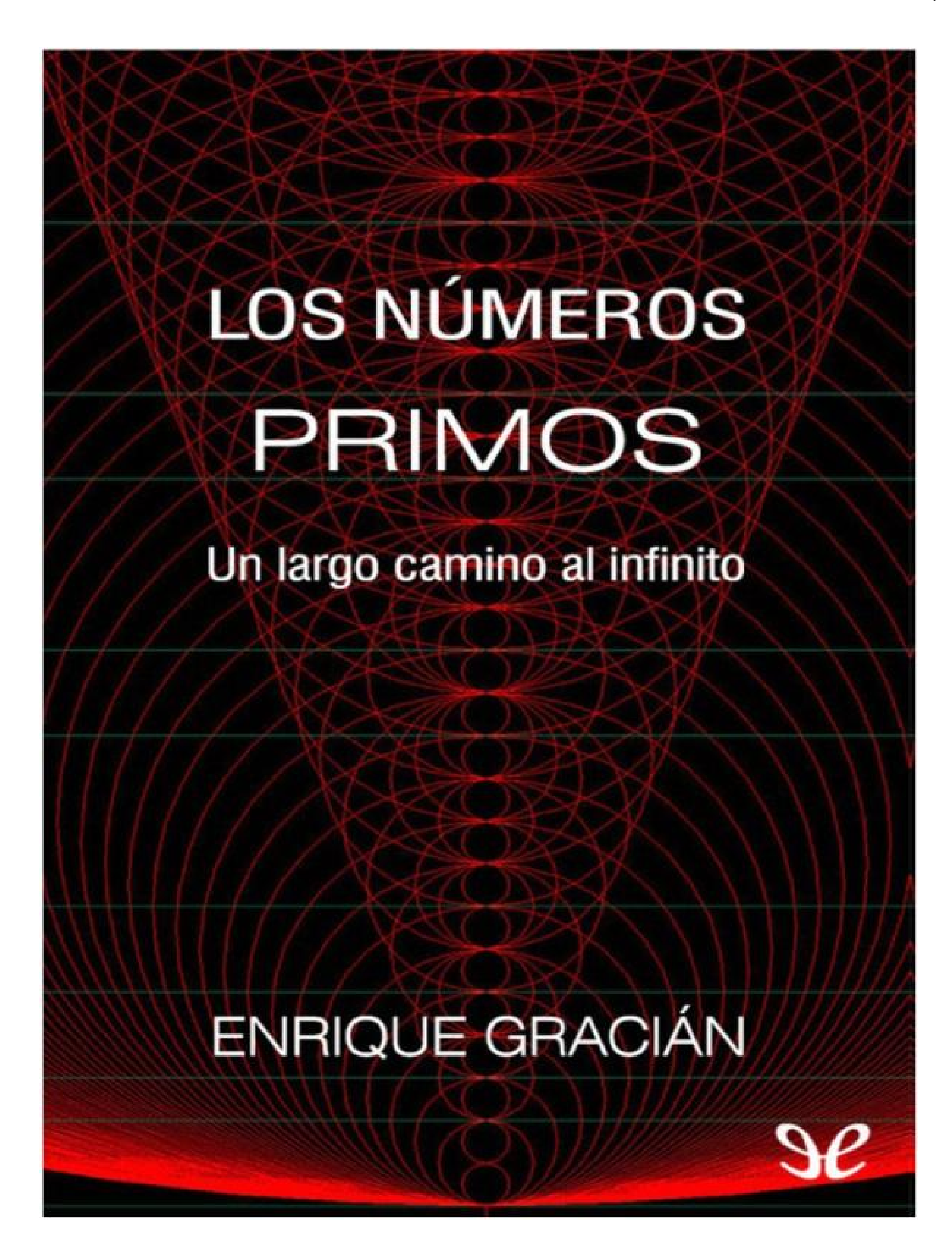

LOS NÚMEROS
PRIMOS
Un largo camino al infinito
ENRIQUE GRACIÁN

Prefacio

La mayoría de los números tienen lo que podríamos llamar un «buen comportamiento» aritmético: los pares se alternan siempre con los impares, los múltiplos de 3 aparecen siempre cada tres números, los cuadrados perfectos siguen una ley de formación fácil de determinar, y de este modo podríamos confeccionar una larga lista de números que hacen lo que se espera de ellos, no importa lo grandes que sean o dónde se encuentren ubicados. Por el contrario, los números primos son un auténtico incordio: aparecen donde quieren, sin previo aviso, de una forma aparentemente caótica, y sin seguir ningún tipo de regla. Y lo peor del caso es que no se pueden ignorar: son la esencia de la aritmética y, hasta cierto punto, de toda la matemática.

En realidad, los números primos no constituyen un concepto complicado que requiera años de estudios matemáticos; de hecho, se enseñan en los colegios, en los primeros cursos de matemáticas.

Para saber lo que es un número primo basta con conocer un sistema de numeración y las cuatro operaciones fundamentales. Sin embargo, han sido y siguen siendo uno de los retos más fabulosos de la historia de la ciencia. Si alguien que quiera dedicarse a las matemáticas no consigue llevarse bien con ellos, está perdido, puesto que siempre están ahí, agazapados para hacer acto de presencia en el momento más inesperado y, cuando aparecen, lo hacen de manera ineludible e implacable, marcando el terreno e imponiendo su fuerza decisoria.

Su influencia no sólo está presente en el universo particular de las matemáticas, sino que, aunque no seamos conscientes de ello, los números primos desempeñan un papel decisivo en nuestra vida cotidiana: en la protección que requiere nuestro ordenador personal, en las transacciones bancarias o en la privacidad de nuestras conversaciones a través de la telefonía móvil, ya que son las piedras angulares de la seguridad informática.

En un sentido metafórico, los números primos son como un virus maléfico que, cuando ataca la mente de un matemático, es muy difícil de erradicar. Euclides, Fermat, Euler, Gauss, Riemann, Ramanujan y una larga lista de los matemáticos de más renombre de la historia cayeron en sus redes. Algunos consiguieron zafarse de

él de manera más o menos exitosa, pero todos ellos sucumbieron a la obsesión por encontrar la «fórmula mágica», una regla de formación que decidiera cuál es el número primo que sigue a un número cualquiera. Sin embargo, ninguno lo consiguió.

A lo largo de la historia de las matemáticas los números primos han ido dejando un extenso rastro de conjeturas. En cierto modo, se podría decir que la historia de los números primos es la historia de un gran fracaso, pero de un fracaso maravilloso que, durante toda su andadura, ha generado nuevas teorías, nuevos paradigmas, nuevos hitos que han marcado un antes y un después. En lo concerniente a creatividad matemática, los números primos han sido una fuente de riqueza tal que, aunque resulte paradójico decirlo, es una suerte que todavía no se hayan dejado dominar. Y todo apunta a que esto seguirá siendo así durante mucho tiempo.

En el desarrollo de la exposición de este libro hemos tratado de mantener un nivel de divulgación «alto», lo que significa que el bagaje de conocimientos matemáticos requeridos para su lectura es «bajo». El entrecomillado de ambos adjetivos responde al hecho de que se trata de conceptos relativos, y más aún si cabe en el tema que nos ocupa. En cualquier caso, este libro puede ser abordado por cualquier lector que sepa lo que son los números y las operaciones básicas que se pueden realizar con ellos, con la intención de que su lectura le proporcione una idea concisa de lo que es el universo de los números primos.

En contrapartida, y pensando en aquellos lectores que posean conocimientos más avanzados de matemáticas, hemos pretendido incluir información de determinados procesos históricos que se revelan esenciales para comprender los vericuetos por los que se han movido los grandes matemáticos de la historia en sus investigaciones sobre los problemas que plantean los números primos.

Para concluir, y como queda de manifiesto desde el primer capítulo, el concepto de número primo y los retos que dichos números plantean son simples y sencillos de explicar, pero las soluciones que se proponen pertenecen, en su mayoría, a las esferas más altas de las matemáticas profesionales.

Capítulo 1
En los albores de la aritmética

Contenido:

1. *Nada hay más natural que un número natural*
2. *¿Qué es un número primo?*
3. *Los números primos, ¿invento o descubrimiento?*
4. *La criba de Eratóstenes*
5. *¿Cuántos números primos hay?*

Los números primos, como todo, tuvieron un origen, un nacimiento que hay que buscar en los mismos inicios de los sistemas de numeración. Vinieron dados con los números naturales, pero muy pronto destacaron como «números especiales».

1. Nada hay más natural que un número natural

«Dios hizo los diez primeros números; el resto es obra del hombre». Leopold Kronecker (1823-1891), matemático alemán a quien se atribuye esta afirmación, se refería a los números naturales, que son los que utilizamos para contar, 1, 2, 3, 4, 5,... Kronecker afirmaba así que gran parte del edificio matemático se construye a partir de la aritmética elemental. Pero afirmar que Dios nos dio los diez primeros números es tanto como decir, fuera de un contexto religioso, que no hay nada más natural que un número natural, es decir, que estos números siempre han estado ahí, como formando parte de la naturaleza que nos rodea.

No sería muy aventurado suponer que el proceso de contar se inició cuando el ser humano abandonó el estado de cazador-recolector para iniciar su larga andadura como agricultor-ganadero.

En ese momento, numerosos bienes, como granos de trigo, cabezas de ganado o recipientes, dejaron de tener un uso inmediato para pasar a ser productos, lo cual hizo necesario iniciar determinados procesos de recuento. Imaginemos a un pastor que saca su rebaño a pastorear.

Necesita estar seguro de que cuando regrese entrarán en el establo tantas cabezas de ganado como salieron. La forma más natural de hacerlo, si no dispone de un

sistema de numeración, es buscar un montón de piedrecillas y colocar en una bolsa una piedra por cada oveja que sale. Luego, al volver, no tiene más que sacar una piedra por cada oveja que entra y comprobar así que las cuentas cuadran. Se trata de un proceso primitivo de cálculo (recordemos que cálculo proviene del latín calculis, «piedra») que no requiere del concepto de número. En términos de matemáticas actuales diríamos que el pastor establece una aplicación biyectiva o biunívoca entre el conjunto de ovejas y el conjunto de piedras. Pensemos que, en matemáticas, el concepto de aplicación biunívoca entre dos conjuntos no se estableció de forma precisa hasta el siglo XIX, por lo que puede resultar paradójico considerar que el proceso de contar sea de lo más natural. Y es que cuando afirmamos que algo es «natural» estamos obligados, por lo menos en este contexto, a establecer algunas precisiones.

Percepción Numérica

Cuando los chinos hablaban de las diez mil estrellas que hay en el cielo, no pretendían haberlas contado todas. Era simplemente una forma de expresar que se trataba de un número muy grande.

Quizás a alguien le parezca que un billón es un número mejor para expresar algo excesivamente numeroso. De entrada hay que tener en cuenta que nuestra percepción directa de un número no va más allá de las cinco unidades. Cuando alguien extiende todos los dedos de una mano y tres de la otra, decimos rápidamente que hay un total de ocho dedos, pero eso es casi un código. Si alineamos ocho objetos encima de una mesa deberemos contarlos o agruparlos en cantidades conocidas para saber cuántos son. Ni que decir tiene que a partir de estas cantidades nuestra percepción sensorial numérica desaparece por completo. Por esta razón es muy difícil que nos hagamos una idea vaga de lo que son un millón de unidades si no tenemos una referencia inmediata. Sabemos el significado que tiene que nos toquen un millón de euros en la lotería porque conocemos el valor del dinero y rápidamente hacemos algunos cálculos de las cosas que podríamos comprar con él. Pero de ahí a que tengamos una percepción clara de lo que supone alinear un millón de monedas de un euro

hay una gran diferencia (cubrirían una distancia de 23,25 km de longitud).



De un único golpe de vista nuestro cerebro es capaz de reconocer como máximo cinco objetos. Con cantidades mayores necesita buscar una estrategia para contarlos.

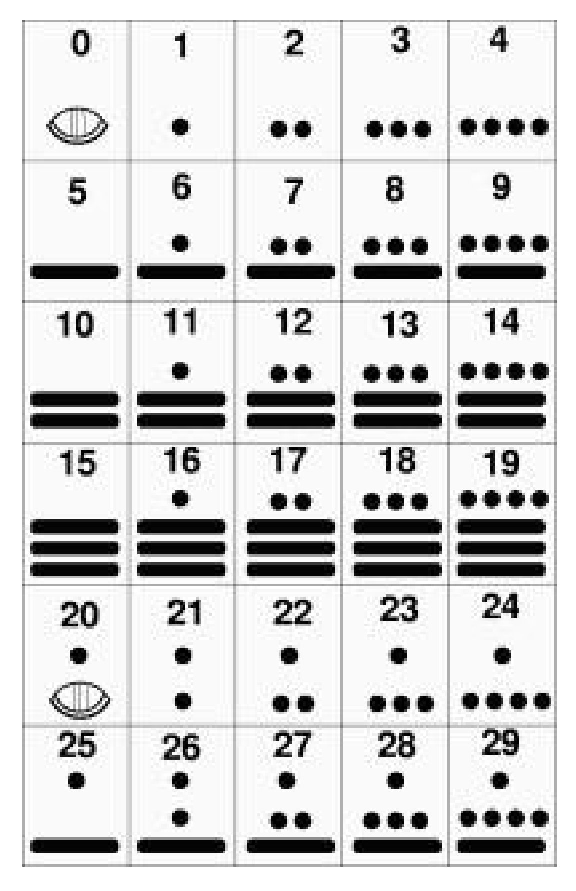
Podríamos entender por natural un proceso mental que surge de forma inmediata, sin necesidad de reflexión previa. Pero no sería del todo cierto que el sistema de conteo con una bolsa llena de piedras no requiera en absoluto de ninguna reflexión previa. En todo caso lo que lo caracterizaría sería su inmediatez en cuanto al uso, a la finalidad práctica que se busca en el proceso. Plantearse el grado de reflexión que conlleva un proceso mental para clasificarlo o no de natural puede ser una tarea demasiado compleja. En este contexto nos resultará más útil hablar de niveles de abstracción.

La introducción de un sistema de numeración conlleva un fuerte proceso de abstracción, hasta el punto de que muchos especialistas consideran que, junto con el aprendizaje del lenguaje, es uno de los mayores esfuerzos mentales que realiza un ser humano a lo largo de su vida. Cuando decimos «tres» nos podemos referir tanto a tres ovejas como a tres piedras, tres casas, tres árboles o tres lo que se quiera. Si tuviéramos que emplear palabras diferentes para numerar cada uno de los objetos a los que nos referimos, la sociedad agrícola-ganadera se habría colapsado en sus inicios. Tres es un concepto abstracto, una pura imagen mental que para subsistir como tal en un grupo social sólo requiere de una palabra y de un signo como vehículos de comunicación.

Recordemos de pasada que el lenguaje cotidiano también conlleva procesos de abstracción. Cuando un niño aprende por primera vez la palabra «silla» se suele

referir exclusivamente al objeto que él utiliza para sentarse, pero poco a poco se va dando cuenta de que la misma palabra puede referirse no sólo a su trona, sino también a muchos otros objetos de la casa cuya función es siempre la misma. El proceso de abstracción continúa y un día aparece la palabra «asiento», un nivel más de abstracción que ya no sólo incluye a las sillas, sino también a los bancos, las tarimas y a cualquier cosa que sirva para sentarse. En este orden de cosas nadie debería dudar de que el proceso evolutivo, en cuanto a especies «inteligentes» se refiere, está inexorablemente unido al progresivo incremento de su capacidad de abstracción.

Mucha gente tiene aversión a las matemáticas, una aversión que justifica aduciendo que son demasiado abstractas, como si el proceso de abstracción fuera algo artificioso, poco natural. Pero esto no es así. Sin acudir a nuestra capacidad de abstracción ni siquiera seríamos capaces de establecer un lenguaje común. A veces, el pensamiento abstracto también suele calificarse de poco práctico, lo cual tampoco es cierto. Cuanto más práctico queremos que sea un método, más elaborado y abstracto debe ser concebido. Un buen ejemplo de ello es el sistema de numeración posicional que utilizamos cada día (de la forma más «natural»). En un sistema de numeración que no sea posicional, el símbolo que representa a un número tiene el mismo valor sea cual sea la posición que ocupe. Por ejemplo, en el sistema de numeración romano el número cinco, que viene representado por la letra V, tiene el mismo valor en las expresiones XV, XVI o VII; en cambio, si el romano hubiera sido como el nuestro, un sistema de numeración posicional, la V equivaldría a cinco unidades en el primer caso, cincuenta en el segundo y quinientas en el tercero.



La cultura maya fue una de las pocas civilizaciones del mundo antiguo que desarrollaron un sistema de numeración posicional. Los mayas tan sólo empleaban tres símbolos: una concha para representar el cero, un punto para la unidad y una raya para expresar cinco unidades.

Crear un sistema de numeración posicional no fue precisamente una tarea sencilla: se tardó más de mil años en conseguirlo. La historia de los números es larga y apasionante, pero no es el tema que nos ocupa. De manera que en nuestro escenario consideraremos que los números ya están ahí y que, además, conocemos las operaciones básicas de suma, resta, multiplicación y división.

2. ¿Qué es un número primo?

Tomemos un número cualquiera, por ejemplo, el 12. Sabemos que podemos expresar este número de diferentes formas como producto de otros números:

$$12 = 2 \times 6$$

12 = 3 x 4

12 = 2 x 2 x 3.

A partir de ahora nos referiremos a estos números como «factores» o «divisores». De manera que diremos que 3 es un factor de 12, al igual que podemos decir que 3 es un divisor de 12. Divisor significa que divide, así 3 divide a 12. De la misma forma decimos que 5 es un divisor de 20, porque 5 divide a 20. Al decir que divide lo que queremos expresar es que si hacemos la división de 20 entre 5 nos da un número natural, en este caso es 4, y que el resto de la división es cero.

La palabra factor también tiene un significado preciso. Viene del latín facere, «hacer» o «fabricar». En la expresión 12 = 3 x 4, el número 3 es un factor porque es un número que permite «fabricar» el número 12.

Según esto, cuando nos preguntamos cuáles son los divisores de 12 podemos contestar que 2, 3, 4, 6 son divisores de 12, pues 12 dividido por cualquiera de ellos da un número exacto. Entre todos los divisores de un número tenemos que contar también con el 1, ya que todo número es divisible por la unidad y también por sí mismo. Por ejemplo, si nos preguntan por qué números es divisible 18, contestaremos que 18 se puede dividir por 1, 2, 3, 6, 9 y 18.

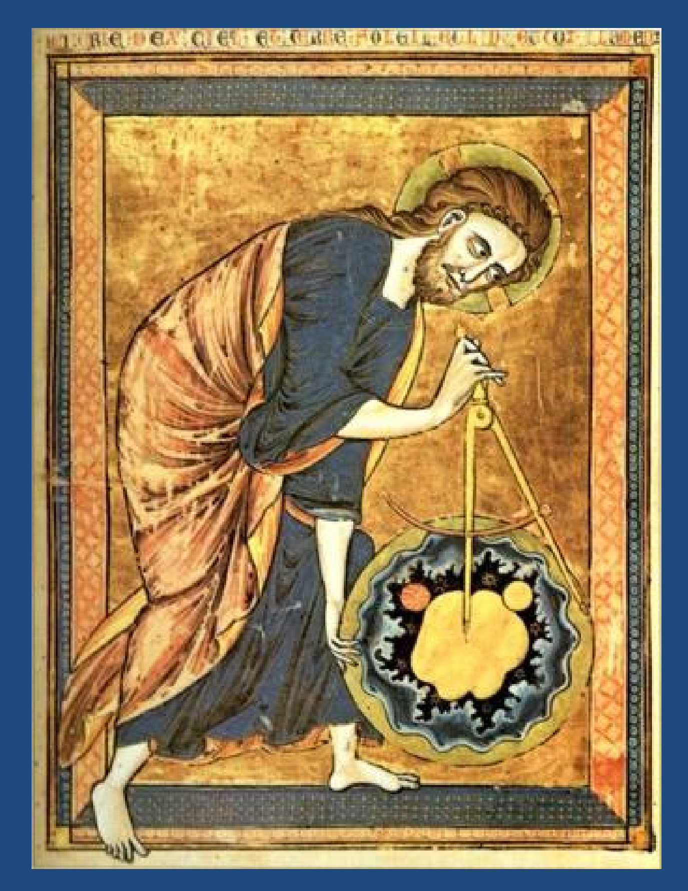
Supongamos que nos formulan la misma pregunta, pero con el número 7. Si buscamos posibles divisores nos encontraremos que los únicos números que dividen a 7 son el 1 y el mismo 7. Algo similar sucede con números como 2, 3, 5, 11 o 13.Y es que todos estos números son «primos».

Signos del Diablo

En las épocas más oscuras de la cultura europea, las cifras eran consideradas como los signos misteriosos de una «escritura secreta», de ahí que, actualmente, aún se siga llamando a los mensajes codificados «mensajes cifrados».

Aunque hablando con propiedad, debería llamarse cifrados a aquellos mensajes en los que las letras han sido sustituidas por números. Cuando

en Europa se introdujeron las primeras cifras árabes en las columnas de los ábacos, los «abacistas» puros las volvieron a sustituir por números romanos.



Gerberto de Aurillac era Silvestre II, el papa matemático.

No podían permitir la presencia de aquellos «signos diabólicos con los que Satanás había pervertido a los árabes». Seis siglos después de la muerte del papa Silvestre II, la Iglesia mandó abrir su tumba para comprobar si todavía permanecían en ella los demonios que le habían inspirado la ciencia sarracena de los números.

Ahora estamos en condiciones de dar una definición precisa de lo que es un número primo: Se dice que un número es primo cuando sólo es divisible por sí mismo y por la unidad.

En esta reflexión sobre los números naturales han intervenido las operaciones de producto y división entre ellos. Hemos llegado a la conclusión de que hay algunos números especiales y, al caracterizarlos a todos mediante una definición, hemos realizado un proceso de abstracción. Tras ponerles un nombre y una propiedad que los define, ya son objeto de estudio.

El teorema fundamental de la aritmética Es frecuente referirse a los números primos como a los «ladrillos» de las matemáticas, los átomos de la aritmética o el código genético de los números. Con los ladrillos se construyen las casas; con los átomos, todos los elementos de la naturaleza; con el código genético, los seres vivos. Todas estas expresiones tienen un significado común: elementos primigenios a partir de los cuales se genera algo, en este caso los números. Veamos cómo se han agenciado este papel los números primos.

Hemos visto que un número podía descomponerse en divisores o factores. Así, el número 12 se puede descomponer en 3 x 4. Recordemos que cuando hablamos de factores estamos pensando en que con los números 3 y 4 podemos fabricar el 12. Sabemos que también lo podríamos fabricar con otros números, por ejemplo:

$$12 = 2 \times 6 = 3 \times 4 = 2 \times 2 \times 3.$$

Todos ellos son «factores» del número 12. A este proceso se le llama «descomponer un número en producto de factores». Recordemos que éste era el criterio que nos había permitido dar una definición precisa de lo que es un número primo: aquel cuyos únicos factores son él mismo y la unidad. Según esto, los únicos factores de un número primo, como el 13, son:

$$13 = 1 \times 13.$$

Cuando en un producto uno de los factores está repetido, ponemos el número con un superíndice que indica el número de veces que éste se repite. Por ejemplo,

$$2 \times 2 \times 2 \times 2 \times 2 = 2^5;$$

$$3 \times 3 \times 3 \times 3 = 3^4$$

Es lo que en matemáticas recibe el nombre de «potencia» y se lee 2^5, dos elevado a cinco, y 3^4, tres elevado a cuatro.

En el ejemplo anterior hemos descompuesto el número 12 en tres productos de factores diferentes: 2 y 6; 3 y 4; 2, 2 y 3. De todos ellos el último es el único que está formado únicamente por números primos.

Veamos otro ejemplo con otro número cualquiera, como el 20:

$$20 = 2 \times 10 = 2 \times 2 \times 5 = 4 \times 5.$$

Sólo la descomposición $20 = 2 \times 2 \times 5 = 2^2 \times 5$ contiene únicamente factores primos.

La pregunta que nos formulamos ahora es: dado un número cualquiera ¿es siempre posible encontrar una descomposición de éste en factores primos? Es decir, ¿puede expresarse como un producto de números que sean todos primos? La respuesta es sí. No sólo eso, sino que únicamente se puede hacer de una manera.

Cómo descubrir los números primos

120	2	*Para hacer una descomposición en factores primos, el método que hay que seguir consiste en colocar el número en cuestión a la izquierda de una línea vertical. Se tantea entonces si el número es divisible por 2, 3, 5, etc., es decir, por números primos empezando por el más pequeño. En el caso de que sea divisible, se coloca el resultado de la división en la parte de la izquierda y se empieza de nuevo con este número. Se sigue el proceso hasta que el número de la izquierda es la unidad. En la columna de la derecha aparecen entonces los números primos que factorizan al número dado.*
60	2	
30	2	
15	3	
5	5	
1		

Cuando escribimos el número 20 como producto de factores primos, $20 = 2^2 \times 5$, lo hacemos de la única manera posible en que se puede hacer (se entiende que el

orden de los factores no interviene, pues es lo mismo 2 - 5 - 2 que 5 - 2- 2). Éste es el teorema, atribuido a Euclides, conocido como «teorema fundamental de la aritmética» y que dice: «Todo número natural se puede descomponer de forma única como producto de factores primos».

De manera que cuando escribimos $24 = 2^3 \times 3$ estamos afirmando que ésta es la única manera posible de hacerlo mediante factores primos. En este caso, el título de «teorema fundamental» está totalmente justificado, pues es, literalmente, uno de los grandes pilares en los que se apoya la aritmética. Además, desde este punto de vista, los números primos adquieren una dimensión trascendental. Volviendo a los símiles anteriores, se podría decir que $2^3 \times 3$ es el ADN del número 24, una cadena formada por los genes 2^3 y 3, o que 2 y 3 son los átomos con los que se forma el elemento 24.

Por consiguiente, los números primos son los elementos primordiales con los que se construyen todos los números. La palabra «primo», que proviene del latín primus, quiere decir «primero» y alude al concepto de «primario», «primitivo», en el sentido de origen, ya que todos los números pueden obtenerse a partir de ellos. De la misma manera que los átomos se unen formando moléculas, los números primos forman números naturales. Todos los elementos químicos conocidos están formados por átomos que se combinan entre sí de formas específicas. Dmitri Ivánovich Mendeleiev (1834-1907) fue el químico ruso creador de la tabla periódica de los elementos, una ordenación en la que están agrupados todos los elementos químicos naturales y también los creados artificialmente. No existe, sin embargo, algo análogo para los números primos, algún tipo de tabla que permita agruparlos siguiendo un criterio, alguna ley de formación a la que respondan sin ambigüedades. Los números primos aparecen como un conjunto caótico, sin orden ni concierto, y se distribuyen de manera aparentemente aleatoria por la serie de los números naturales.

3. Los números primos, ¿invento o descubrimiento?

Una vez establecido un sistema de numeración parece lógico que la primera propiedad que se detectara en un número fuera la de ser par o impar, un concepto muy intuitivo e inmediato. El siguiente paso era plantearse la factorización de

números, lo que lleva a establecer los criterios de divisibilidad que se enseñan en los colegios a una edad temprana. De esta forma, una cultura que haya establecido su sistema de numeración tiene una colección de números controlados por unas pocas propiedades fáciles de establecer. Todos excepto los números primos. Lo único que se sabía a ciencia cierta de estos números es que no pueden ser pares, ya que entonces serían divisibles por dos. Tampoco cabía tratarlos como una rareza difícil de descubrir, ya que Euclides había demostrado que eran infinitos (más adelante detallaremos el elegante modo del que se valió para ello). Y no era posible subestimar su importancia, pues el teorema fundamental de la aritmética los había situado en el cuadro de honor de las matemáticas. Por consiguiente, y como ya hemos dicho, se habían constituido en objeto de estudio.

Cuando en las ciencias experimentales se habla de un objeto de estudio parece claro que dicho objeto está ahí fuera, en alguna parte. Podemos haberlo descubierto o no y, a continuación, dedicarnos a investigarlo o a ignorarlo, pero en cualquier caso sigue ahí, independientemente de lo que pensemos o hagamos con él. A partir de cierto momento, las bacterias fueron objeto de estudio para los biólogos. Nadie pone en duda que ya estaban presentes en los organismos vivos antes de que existieran los biólogos, incluso mucho antes de que surgiera la especie humana. Esto es algo que nadie se cuestiona en ningún ámbito científico. Sin embargo, en matemáticas es un tema que adquiere un cariz diferente. Los números primos ¿son un invento o un descubrimiento?

¿Existirían los números primos si no existieran los seres humanos? Esta discusión ha generado y sigue generando mucha polémica, para algunos apasionante y para otros intrascendente. Lo más probable es que sea una pregunta sin respuesta ante la cual sólo podemos acceder a posicionarnos.

Lo realmente importante, en cuanto a la naturaleza de la mente matemática, es que el creador actúa como si fuera un explorador que se adentra en parajes extraños, como si las matemáticas realmente estuvieran fuera de él. Este sentimiento de aventura forma parte de la misma esencia de la investigación matemática y es lo que le imprime su carácter como arte. El físico alemán Heinrich Rudolf Hertz (1857-1894) se preguntaba al respecto: «¿Puede uno evitar sentir que esas fórmulas matemáticas tienen una existencia independiente y una inteligencia propia, que son

más sabias de lo que somos nosotros, más sabias incluso que sus descubridores, y que obtenemos de ellas más de lo que originalmente pusimos en ellas? ».



La universalidad de las matemáticas plantea la duda de si éstas tienen una existencia independiente, al margen del ser humano. Tal reflexión no fue ajena al físico alemán Heinrich Rudolf Hertz.

La corriente filosófica, o mejor, epistemológica, que acepta el hecho de que los objetos (e incluso las verdades matemáticas) existen por cuenta propia recibe la etiqueta de «platonismo», que en resumen viene a decir que sólo se puede mantener una postura objetiva en la medida en que se esté en presencia de objetos.

El hueso de Ishango

Este hueso es probablemente un peroné de babuino con una aparente forma de herramienta; es como un mango que se puede asir fácilmente y que tiene en su extremo un afilado cristal de cuarzo. Fue hallado en las

cercanías del nacimiento del Nilo, entre las fronteras de Uganda y la República Democrática del Congo, y pertenecía a una sociedad tribal que quedó sepultada por una erupción volcánica. La antigüedad del hueso se estima en unos 20.000 años.

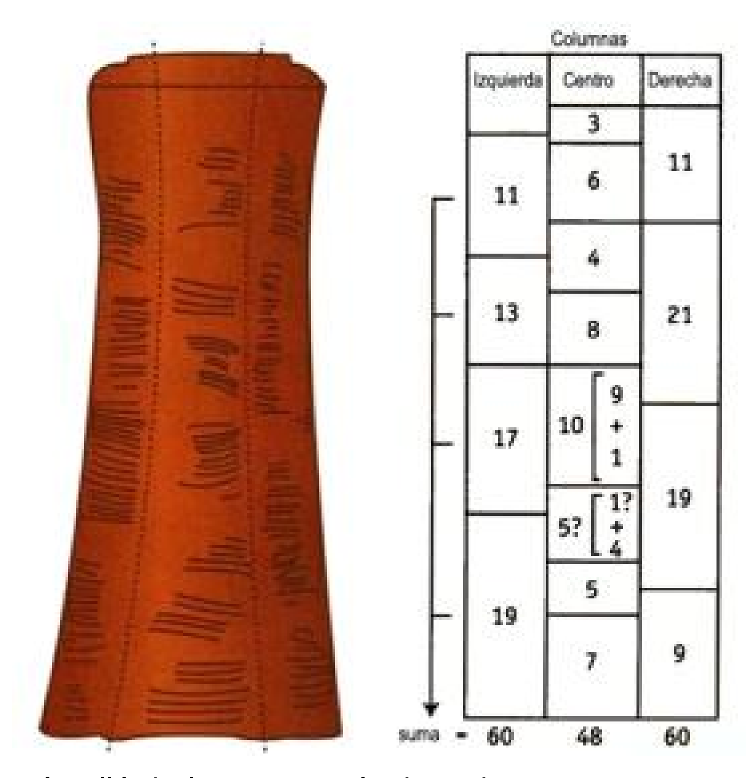


El hueso de Ishango está expuesto en el Museo de Ciencias Naturales de Bruselas, Bélgica.

El esquema muestra la distribución de las muescas, repartidas en tres columnas, en el llamado hueso de Ishango, una herramienta que podría haber servido para hacer cálculos matemáticos sencillos.

Los historiadores de la matemática suelen inclinar la balanza hacia el platonismo basándose en el hecho incuestionable de su universalidad, pues en culturas muy alejadas en el espacio y en el tiempo, las reflexiones matemáticas llegan a las mismas conclusiones, a las mismas verdades objetivas. En el caso de los números primos, por ejemplo, se tiene un dato interesante, que podríamos calificar de arqueología matemática: el hueso de Ishango.

En el hueso pueden apreciarse unas muescas a modo de pequeños segmentos rectilíneos. Un examen más detallado de las mismas llevó a pensar que más que una herramienta se trataba de un sistema de numeración que permitía contar. En ese caso, es probable que la punta de cuarzo sirviera para anotar de algún modo el estado de las cuentas. Dicho de otra manera, el mango de hueso podría hacer las funciones de una primitiva tabla de calcular. La distribución de muescas en esta columna sugiere operaciones de suma y producto en un sistema de numeración en base 12.

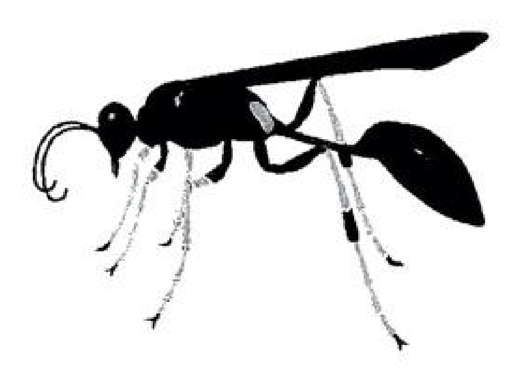


Los números de la derecha son todos impares, pero lo realmente asombroso es que todos los de la izquierda son primos, concretamente los comprendidos entre 10 y 20. Sería muy imprudente atribuir la distribución de estas muescas al puro azar o a cualquier otra función que no implicara un cálculo numérico avanzado. Recordemos que el concepto de número primo requiere de un proceso de abstracción que va más allá de las meras técnicas de recuento.

A la cuestión sobre si las verdades matemáticas existen o no al margen del ser humano se sumaría una tercera postura, una solución conciliadora que considera la posibilidad de admitir que sí existen esos objetos matemáticos susceptibles de ser descubiertos, pero que se trata de «objetos mentales» que heredamos con el paquete genético. De ser así debería existir en la naturaleza alguna forma primitiva de estas configuraciones.

Por lo que respecta a la capacidad de contar, en el reino animal se encuentran numerosos ejemplos de especies que pueden hacerlo con bastante precisión. Las avispas solitarias, por ejemplo, son capaces de contar el número de orugas vivas

que dejan como alimento para sus larvas en las celdillas en las que han puesto los huevos: siempre son exactamente 5, 12 o 24. Entre las pertenecientes al género Eumenes, nos encontramos con un caso aún más asombroso: la avispa sabe si surgirá un macho o una hembra del huevo que ha puesto. No tenemos conocimiento de cuál es el mecanismo del que se vale para averiguar el género de su descendencia, ya que las celdas en las que lleva a cabo la puesta y deposita el alimento no presentan signos distintivos aparentes. El caso es que la avispa deja 5 orugas por cada huevo correspondiente a un macho y 10 si se trata de una hembra. La razón de esta disparidad reside en que las avispas hembras tienen un tamaño muy superior al de los machos.



Las hembras de las avispas solitarias ponen los huevos en unas celdillas en las que también incluyen diversas orugas que previamente dejan paralizadas para que, tras la eclosión, las larvas de avispa se alimenten de ellas.

Lo sorprendente es que estas avispas siempre dejan el mismo número de orugas, y tienen en cuenta si del huevo resultante nacerá un macho o una hembra, pues de ello depende también el número de «victimas» que procuran a su descendencia.

Incluso para un concepto más elaborado, como el de número primo, existe un curioso ejemplo, unas especies de cigarras denominadas *Magicicada septendecim* y M. *tredecim*. Los nombres específicos *septendecim* y *tredecim*, significan, respectivamente, 17 y 13, y hacen referencia a los ciclos vitales de ambas cigarras. Los dos son números primos y los zoólogos han especulado con diferentes teorías que expliquen la elección de un número primo de años para el ciclo vital de estos insectos.

Tomemos como ejemplo *Magicicada septendecim*. Esta cigarra vive como ninfa bajo tierra y se alimenta de la savia que succiona de las raíces de los árboles. Se pasa en ese estado 17 años y luego sale a la superficie para convertirse en insecto adulto, etapa que tan sólo dura unos días, durante los cuales se reproduce y, finalmente, muere. La teoría que explica tal comportamiento es la siguiente: entre los enemigos de la cigarra adulta existe un parásito cuyo ciclo vital es de dos años. Si el ciclo vital de la cigarra fuera un múltiplo de 2, ambas especies acabarían coincidiendo cada 2, 4, 8,... años. Lo mismo sucedería con otros múltiplos cualesquiera. Pero si el ciclo vital es un número primo de años lo suficientemente alto, como es el caso de 17, el parásito y la cigarra sólo pueden coincidir cada 34 años, que es el primer múltiplo de 17. En el hipotético caso de que el ciclo vital del parásito fuera de 16 años, la probabilidad de encontrarse tendría lugar cada 16 x 17 = 272 años.

Es muy posible que, con el tiempo, el estudio del comportamiento animal acabe dando más ejemplos de especies que «sepan contar». No se puede pasar por alto la banalidad de estos razonamientos, pero lo importante del asunto es que aunque los objetos matemáticos, como los números primos, sean una creación humana, el investigador puede llegar a vivirlos y sentirlos como si tuvieran una existencia propia.

4. La criba de Eratóstenes

Generar números primos ha sido y sigue siendo un tema verdaderamente espinoso. Uno de los primeros métodos conocidos para tal cometido se atribuye a Eratóstenes de Cirene (273-194 a. C.), matemático, astrónomo y geógrafo griego que fue director de la biblioteca de Alejandría. Dicho método se conoce como la «criba de Eratóstenes». Veamos cómo se lleva a cabo la criba de los cien primeros números naturales.

En primer lugar se construye una tabla con todos los números naturales del 1 al 100. Se empieza por eliminar todos aquellos que son múltiplos de dos: 4, 6, 8, 10,...; después los que son múltiplos de tres: 6 (ya eliminado), 9, 12, 15,... Le seguirían los múltiplos de cinco y luego los de siete.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~

11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	~~53~~	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	~~89~~	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Los números que han quedado sin eliminar son todos primos.

Obsérvese que la criba finaliza cuando se llega al número 10, que es la raíz cuadrada de 100. En general, para encontrar todos los primos menores que un número N dado, basta con realizar la criba para los números menores o iguales a $\sqrt{N}$. Esto nos proporciona un método para encontrar primos menores que otro dado. Dicho método se sigue utilizando actualmente, más de dos mil años después de su creación, para encontrar primos pequeños, menores que diez mil millones.

Las dimensiones de la tierra

El nombre de Eratóstenes está ligado a la criba de números primos que lleva su nombre. Sin embargo, no fue éste, ni mucho menos, su trabajo más impórtame. De hecho, Eratóstenes ha pasado a la historia de la ciencia por ser el primero que calculó las dimensiones de la Tierra. Con los medios técnicos de que se disponía en el siglo III a. C., fue capaz de calcular la circunferencia polar con un error inferior al 1%.

Planisferio que muestra el mundo conocido según Eratóstenes. El sabio griego fue el primero en utilizar una división en paralelos regulares, aunque los meridianos están separados irregularmente.

5. ¿Cuántos números primos hay?

Si queremos empezar a reflexionar sobre la naturaleza de los números primos para buscar una relación entre ellos o una regla que nos permita predecir en qué momento aparecerá el siguiente, en primer lugar es preciso disponer de una buena colección de ellos. La siguiente lista, obtenida mediante la criba de Eratóstenes, muestra los números primos que se encuentran entre los mil primeros números naturales.

Un examen preliminar nos permite constatar que los números primos son absolutamente impredecibles. Hay, por ejemplo, más primos entre 1 y 100 que entre 101 y 200. Entre los números 1 y 1.000 hay 168 primos. Podríamos pensar que si nuestra tabla fuera mucho más grande veríamos cómo la cantidad de números primos va aumentando a medida que avanzamos de mil en mil unidades. Pero no. Actualmente existen tablas enormemente grandes y se sabe que, por ejemplo, entre las mil unidades que van de 10^{100} y 10^{100} + 1.000 sólo hay 2 números primos. ¡Y estamos hablando de números de más de cien cifras!

2	3	5	7	11	13	17	19
23	29	31	37	41	43	47	53
59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131
137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263
269	271	277	281	283	293	307	311
313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457
461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569
571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719
727	733	739	743	751	757	761	769
773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881
883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997

Parece claro que para poder encontrar una pauta, lo mejor sería disponer de una tabla donde estuvieran todos. ¿Todos? ¿Y si son muchos? No importa, con los medios con que contamos actualmente es posible someterlos a todo tipo de cribas y test que permitan encontrar la pauta. Porque está claro que cuando se trata de conjuntos finitos, por muy grandes que sean, puede acabar encontrándose una pauta o, por lo menos, puede inventarse una que encaje. Pero la cosa cambia, y mucho, cuando se trata de conjuntos infinitos. Por consiguiente, es preciso decidir si hay o no hay infinitos números primos. Ésta es una cuestión que fue propuesta también por Euclides. Su manera de resolverla es tan ingeniosa y matemáticamente sencilla que vale la pena estudiarla con cierto detalle.

Partamos de una pequeña lista de números primos consecutivos, por ejemplo 2, 3, 5.

A continuación, hagamos el producto de todos ellos: 2 x 3 x 5 = 30.

Ahora le sumamos una unidad al resultado: 2 x 3 x 5 + 1 = 30 + 1 = 31.

Está claro que 31 dividido por cualquiera de los números primos de la lista 2, 3, 5 tiene que dar como resto 1:

31/2 = 15 con resto 1; 15 x 2 + 1 = 31.

31/3 = 10 con resto 1; 3 x 10 + 1 = 31.

31/5 = 6 con resto 1; 5 x 6 + 1 =.31

Esto garantiza que no es divisible por ninguno de ellos. Es algo que sucede siempre: si partimos de una lista de números primos consecutivos, cuando los multiplicamos entre sí y añadimos una unidad al resultado, el número obtenido no es divisible por ninguno de los de la lista. Este sencillo hecho es el corazón de la demostración de Euclides.

El número 31 es un número primo que no se encontraba en la lista original, por lo que ésta no estaba completa. Tomemos, por ejemplo, la siguiente lista:

{2, 3, 5, 7, 11, 13}.

Hacemos el producto de todos ellos y sumamos una unidad:

2 x 3 x 5 x 7 x 11 x 13 + 1 = 30.030 + 1 = 30.031.

Éste no es un número primo, ya que puede obtenerse como el producto de dos números: 30.031 = 59 x 509.

Euclides ya había demostrado que todo número natural puede descomponerse de forma única como producto de factores primos. Si aplicamos este resultado al número 30.031, que es un número compuesto, está claro que con los primos de la

lista {2, 3, 5, 7} no tenemos suficiente para hacer la descomposición en factores, por lo que en dicha lista faltan números primos.

La conclusión es la siguiente: por larga que sea la lista original de números primos, al efectuar la operación de multiplicarlos todos entre sí y añadir una unidad, el resultado es un nuevo número que se encuentra en una de las dos situaciones siguientes:

1. Es un número primo que no estaba en la lista.
2. Es un número compuesto en cuya descomposición deben figurar números primos que no estaban en la lista.

De manera que la lista siempre es incompleta a menos que sea infinita.

Desgraciadamente, éste no es un método para obtener números primos, aunque constituye un punto de partida muy importante, ya que proporciona una dimensión del problema y una perspectiva sin la cual sería imposible plantearse estrategia alguna. Podríamos pensar que tampoco es tan importante demostrar que existen infinitos números primos, pues es algo que ya se intuye. Sin embargo, con los números primos hay que tener mucho cuidado, pues son tan «raros» que podría suceder que en algún momento se acabaran. Sin embargo, el teorema de Euclides nos garantiza que eso no sucederá.

Capítulo 2
La esquiva pauta de los números primos

Contenido:

1. *El genio, en contexto*
2. *Los «centros de información»*
3. *Grandes lagunas*
4. *El sentido del ritmo*
5. *Primos gemelos*
6. *Magia y matemáticas*

Como ya hemos comentado con anterioridad, el de los números primos es uno de esos temas mayores cuyo estudio nos remite a los inicios mismos de la matemática y nos conduce, en un recorrido de creciente complejidad, hasta la cresta de la ola de la ciencia contemporánea. Es por ello por lo que resulta una hebra muy valiosa a la hora de desmadejar la fascinante e intrincada historia de la disciplina, muy en particular del modo en que ésta ha ido creciendo, es decir, de cómo se ha ido construyendo el conjunto de verdades aceptadas que la constituyen.

En el presente capítulo veremos cómo sucesivas generaciones de matemáticos escudriñaron el universo de los números en busca de una pauta en la aparición de los primos (una pauta que, no obstante, se hacía más y más esquiva), y también examinaremos con mayor detalle cuestiones relativas al contexto histórico en que dichas figuras trabajaron, y hasta qué punto este trabajo se confundía con prácticas de tipo místico y cuasi religioso en una curiosa síntesis que poco se parece al ideal científico que prevalece hoy día. Laboriosa y tentativamente, se abonaba el terreno para nuevos paradigmas, como los que impulsarían Fermat o Euler en los siglos XVII y XVIII y que se tratan con detalle en el próximo capítulo.

1. El genio, en contexto

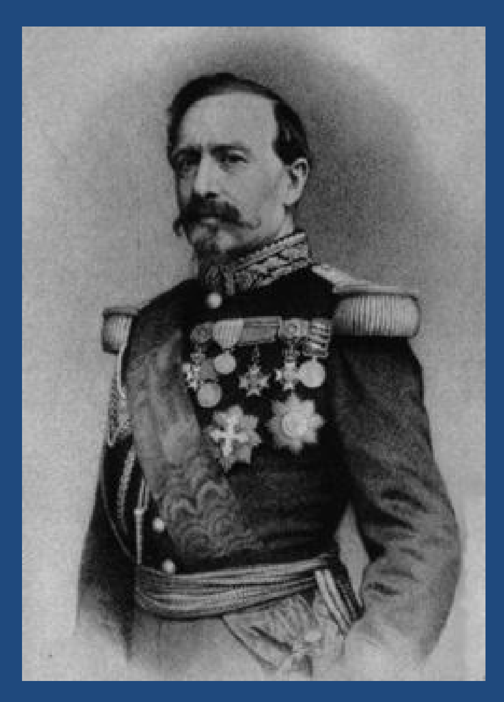
Como en toda historia de la ciencia, en la de los números primos aparecen nombres propios adscritos a grandes descubrimientos. Pero estos personajes no existirían sin un tejido cultural que les sirviera de apoyo, ya que los «genios» no nacen de la

nada, sino que surgen en caldos de cultivo adecuados. De ahí la importancia de reparar tanto en los paradigmas que genera el tejido cultural como en las organizaciones sociales que han servido de vehículo para que el desarrollo científico pudiera seguir avanzando.

En la década de 1930 empezaron a aparecer en las librerías especializadas una serie de libros de matemáticas que estaban firmados por Nicolás Bourbaki, un autor hasta entonces desconocido. Fue una colección de textos que obtuvo cierto éxito entre la comunidad matemática debido, entre otros motivos, a que permitió a los estudiantes disponer de un buen tratado de análisis matemático que hasta entonces no existía.

El general matemático

¿De dónde surgió el nombre de Bourbaki? Según la versión de uno de sus más destacados miembros, André Weil, la idea surgió de una anécdota de sus tiempos de estudiante.



El general Denis Bourbaki, inspiración de patriotas y matemáticos.

Al parecer, Cartan y Weil, entre otros, acudieron a un seminario celebrado

por un oscuro matemático de nombre vagamente nórdico, acento indefinible y aspecto estrafalario, durante el cual se enunció un teorema de Bourbaki, de contenido tan pasmoso como increíble, y que supuestamente se debía al oficial francés Denis Bourbaki (1816-1897), una figura célebre de la guerra franco prusiana. El seminario en su totalidad resultó ser la monumental travesura de un estudiante, Raoul Husson, pero Cartan y Weil encontraron en la figura de este general, matemático a su pesar, y en su apellido de inspiración griega, el seudónimo perfecto bajo el que presentar su particular «reconstrucción euclidiana» de las matemáticas.

Pero su objetivo no fue únicamente el de proveer al mercado de nuevos libros de texto, sino básicamente el de conseguir unificar criterios en algunos sectores de las matemáticas, como el álgebra o el análisis, en los que imperaba un cierto caos debido a la ingente cantidad de nuevos resultados que se habían obtenido en los últimos años. Fue una sorpresa para muchos descubrir que en realidad nunca existió un matemático llamado Nicolás Bourbaki, sino que éste fue el nombre que eligió un grupo de matemáticos, entre ellos Henri Cartan (1904-2008) y André Weil (1906-1998), para llevar a cabo una reconstrucción de las matemáticas, animados, eso sí, por un espíritu totalmente filantrópico. El grupo Bourbaki está lo suficientemente documentado, ya que se trata de un hecho reciente. No sucede lo mismo con otros posibles grupos abanderaron bajo un nombre común.

2. Los «centros de información»

Lo remarcable es el hecho de que el conocimiento científico en general y el matemático en particular nunca se deben a la mano de una sola persona. Sí es cierto que a algunas de ellas se les atribuyen grandes descubrimientos, pero han surgido en el seno de una comunidad matemática.

Ello requiere la existencia de escritos, escuelas, lugares de reunión y centros con capacidad de aglutinar información y de establecer redes de comunicación entre los científicos. Actualmente, las posibilidades de comunicación han alcanzado las cotas más altas de la historia de la Humanidad. La comunicación *on line* permite poner un descubrimiento o avance científico al alcance de cualquiera que desee tener acceso

a él, y, además, de forma inmediata. Sin embargo, la necesidad de almacenar información para que otros la puedan utilizar es algo común a cualquier época de la historia; es lo que constituye el legado cultural de una sociedad. En este aspecto, los números primos son un objeto de investigación singular. Están siempre en todas partes. Son los protagonistas de una obra que empieza en la noche de los tiempos y que todavía no ha finalizado. Seguir su rastro no sólo aporta información sobre su naturaleza matemática, sino que también permite asistir a la evolución de estos espacios de encuentro a los que, empleando una terminología moderna, podríamos calificar de «centros de información». El caso de la biblioteca de Alejandría es, en este sentido, un ejemplo paradigmático.

Alejandría

Ptolomeo I Sóter, fundador y primer rey de la Dinastía Ptolemeica, estableció la capital de Egipto en Alejandría. Rodeado de los mejores arquitectos del mundo, convirtió la ciudad en una maravilla arquitectónica. Tendió un largo puente hasta la isla de Faros y construyó allí una torre que durante mil años sirvió de guía a los navegantes del Mediterráneo. Luego fundó una biblioteca cuya fama ha permanecido a través de los tiempos. Un faro y una biblioteca eran los dos elementos necesarios para que Alejandría se convirtiera en el centro de información más importante del mundo antiguo, un objetivo que Ptolomeo estaba dispuesto a conseguir costara lo que costara. Su primer paso fue rescatar del exilio a Demetrio, un tirano al que Casandro, uno de los tres herederos de Alejandro, había nombrado gobernador de Atenas. Demetrio había sido quien había mantenido viva la fundación del Liceo creado por Aristóteles. A pesar de haberse dedicado a las intrigas del poder, la verdadera vocación de Demetrio era el conocimiento, por lo que recibió de muy buen agrado la invitación de Ptolomeo para fundar en Alejandría una biblioteca capaz de agrupar y clasificar en un único centro todo el saber del mundo civilizado.

El puerto de Alejandría estaba formado por pequeñas islas protegidas por diques y con una única salida al mar, que era el gran canal por el que entraban y salían los navíos. La protección frente a los intrusos era prácticamente total. Uno de los barrios más importantes a los que se podía acceder era el Brucheion, en pleno corazón de la ciudad, que albergaba los palacios más importantes, entre ellos el

dedicado a las Musas, el «Museo», consagrado a la música y las ciencias, es decir, a las melodías, los ritmos y los números. Cuando Demetrio fue consciente de que aquel centro de conocimiento estaba respaldado por uno de los reyes más poderosos del mundo conocido, no dudó ni un instante en responsabilizarse de su dirección. Lo primero que hizo fue solicitar de Atenas que le prestaran los textos de los pensadores y literatos más importantes que había producido la cultura helénica hasta el momento. Los hizo copiar, devolvió las copias a Atenas y puso los originales junto a los otros textos que Ptolomeo había conseguido como botines de guerra a lo largo de sus campañas. El método para ir ampliándola se reveló muy eficaz, aunque también nada ortodoxo: a cada barco que recalaba en el puerto de Alejandría se le requisaban todos los originales que llevaba a bordo para ser copiados; éstos ingresaban en la biblioteca y las copias se devolvían a los barcos. Fue así como nació la llamada «biblioteca de los bajeles». Pero aquellos que detentaban el poder y las riquezas del Mediterráneo pronto se dieron cuenta de la jugada, con el consiguiente rechazo. Demetrio ofreció entonces un incentivo a los mercaderes: si querían negociar con las enormes riquezas que les ofrecía el puerto de Alejandría debían traer, a modo de salvoconducto, manuscritos procedentes de sus puertos de origen: no importaba que fuesen tratados de ingeniería, filosofía, arte, matemáticas o música, mientras supusieran un aporte de conocimiento. El trato era que se harían copias, los originales se quedarían en la biblioteca y las copias serían devueltas a los mercaderes. Éstas eran guardadas en los estuches originales y la mayoría de los propietarios no notaban la diferencia, y cuando se percataban del cambio parecía no importarles demasiado. Ha quedado constancia histórica de que, en aquel entonces, Alejandría dio trabajo al mayor plantel de copistas conocido hasta el momento.

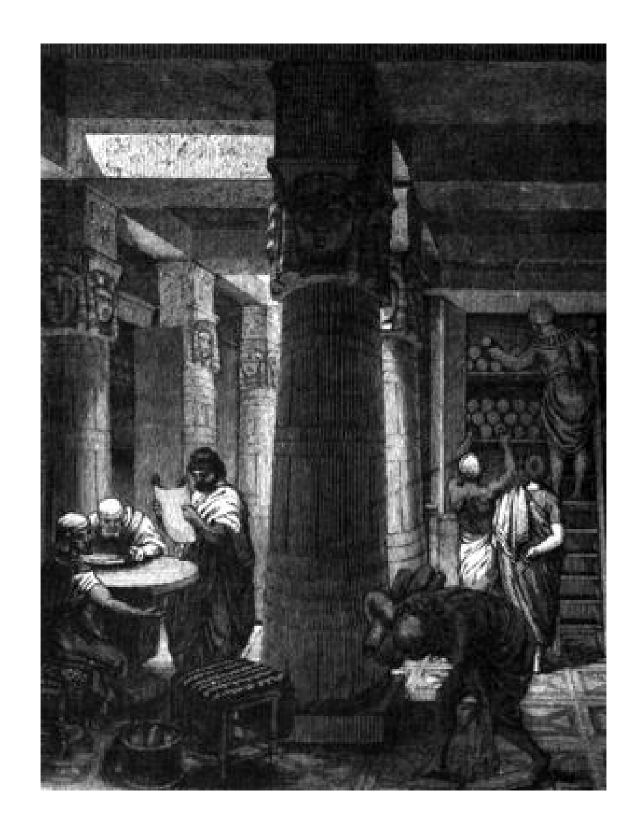


Monedas romanas acuñadas con la imagen del faro, otra de las maravillas de la ciudad.

Pero Alejandría no era solamente un centro donde se almacenaban «archivos de información», sino que constituía asimismo un lugar en el que se ésta se «gestionaba». Pronto atrajo a numerosos maestros de todas las disciplinas que impartían sus clases y compartían su saber con otros condiscípulos. Para tal propósito se construyeron aulas, celdas de alojamiento, pórticos y paseos ajardinados.

Es razonable pensar que se formaran diferentes escuelas a lo largo del tiempo, entre ellas, por qué no, la escuela de Euclides, la cual, de forma similar al grupo Bourbaki, reunió el saber matemático conocido hasta entonces para convertirlo en una escuela de pensamiento, es decir, en una forma de pensar y de hacer matemáticas cuyos frutos han perdurado hasta nuestros tiempos.

Tengamos en cuenta de que dos mil años después se sigue enseñando en las escuelas exactamente la misma geometría que nació entre las aulas y los jardines de Alejandría.



Alejandría fue el centro de información más importante de la Antigüedad. El grabado ilustra una escena en el interior de la famosa biblioteca.

3. Grandes lagunas

Lo primero que llamó la atención a los antiguos matemáticos en relación a los números primos es la ausencia de pautas en cuanto a su aparición en la sucesión de los números naturales. Y no sólo eso, sino que resulta que tampoco tienen un comportamiento claro por lo que respecta a su ausencia, es decir, la manera en que dejan de aparecer. Por consiguiente, pueden estar relativamente juntos o, por el contrario, distanciarse muchísimo. Si tenemos en cuenta, por ejemplo, los números primos que hay entre los cien primeros números naturales, 2, 3, 5, 7, 11,13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, observaremos que los ocho primeros aparecen muy seguidos, hay ocho entre los veinte primeros y, en cambio, no hay ninguno entre el 89 y el 97.

Si tomamos los números primos comprendidos entre 100 y 200, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, veremos grandes lagunas, como los nueve números compuestos seguidos desde el 182 hasta el 190.

La pregunta que surge entonces es: ¿Puede haber lagunas muy, muy grandes, como, por ejemplo, cincuenta mil números seguidos entre los que no haya ningún número primo?

El universo de los números primos es lo suficientemente vasto como para poder encontrar en él enormes lagunas. Es decir, series tan largas como queramos de números seguidos que no sean primos. No se trata de una mera conjetura, sino que se deriva un resultado sencillo de demostrar.

Consideremos el producto de los cuatro primeros números naturales:

$$1 \times 2 \times 3 \times 4$$

Podemos asegurar que el número 1 x 2 x 3 x 4 + 2 no puede ser primo porque es divisible por 2. La comprobación es inmediata, ya que 1 x 2 x 3 x 4 + 2 = 24 + 2 = 26, y al dividirlo por 2 da 13.

No era necesario hacer ninguna operación para saber que era divisible por dos, ya que los dos sumandos contienen el número 2.

Por la misma razón se tiene que

1 x 2 x 3 x 4 + 3 no puede ser primo porque es divisible por 3;

1 x 2 x 3 x 4 + 4 no puede ser primo porque es divisible por 4.

De esta forma hemos obtenido tres números consecutivos, 26, 27, 28, que no son primos. Si ahora queremos obtener cuatro números consecutivos que no sean primos hacemos:

1 x 2 x 3 x 4 x 5 + 2 = 122;

1 x 2 x 3 x 4 x 5 + 3 = 123;

1 x 2 x 3 x 4 x 5 + 4 = 124;

1 x 2 x 3 x 4 x 5 + 5 = 125.

Para mayor comodidad, representaremos el producto de números consecutivos con un signo de admiración:

1 x 2 x 3 x 4 = 4!;

1 x 2 x 3 x 4 x 5 = 5!

En matemáticas, este tipo de expresiones reciben el nombre de «factoriales». Por ejemplo, el factorial de 6 es

6! = 1 x 2 x 3 x 4 x 5 x 6 = 720.

Por consiguiente, es más cómodo escribir las anteriores expresiones de la forma siguiente:

5! + 2;

5! + 3;

5! + 4;

5! + 5.

De este modo, podemos escribir series de números consecutivos que no contengan ningún número primo. Por ejemplo, si queremos escribir cien números consecutivos de manera que ninguno de ellos sea primo, no tenemos más que hacer lo siguiente:

101! + 2;

101! + 3;

101! + 4,

y así hasta 101! + 101.

Esto quiere decir que hay grandes lagunas en las que no aparecen números primos. Por el mismo método podríamos construir una serie de cinco trillones de números seguidos en la que no apareciera ningún número primo. Ello induce a pensar que los números primos escasean cada vez más a medida que avanzamos en la sucesión de los números naturales, y por consiguiente, a medida que nos vayamos alejando hacia el infinito llegará un momento en que ya no habrá ninguno más.

Esta tentadora idea responde a una falsa intuición, ya que sabemos que el teorema de Euclides garantiza que hay infinitos números primos y que, por muy larga que sea una serie de números compuestos, en algún momento volverá a aparecer un número primo.

El uso de la calculadora

Es tentador plantearse programas que faciliten el cálculo de grandes

lagunas de números primos mediante computación. De hecho, el algoritmo serla bastante sencillo, pero hay que tener en cuenta que cuando se manejan números factoriales los cálculos computacionales hay que olvidarlos. Los factoriales crecen a velocidad de vértigo. Se puede hacer una prueba en cualquier calculadora de bolsillo que disponga de esta tecla, que son la mayoría (recordemos que el símbolo es !), Tan sólo con los primeros números se obtiene lo siguiente:

1! = 1	*2! = 2*	*3! = 6*
4! = 24	*5! = 120*	*6! = 720*
7! = 5.040	*8! = 40.320*	*9! = 362.880*
10! =3.628.800.		

Muchas de estas calculadoras dejan de realizar esta función a partir del número 70

4. El sentido del ritmo

Hay una situación que suele darse en algunos conciertos, en los que el público se anima y bate palmas al ritmo de la música. Al principio la cosa parece que funciona, pero al cabo de poco rato empieza a haber una falta de sincronía entre el ritmo que marca el público asistente y el que intenta mantener el percusionista. La situación puede mantenerse más o menos estable en el caso de ritmos sencillos, pero es impensable cuando se trata de ritmos más complicados. Nos podemos valer de esta analogía para comprender el esfuerzo de los matemáticos a la hora de imponer un ritmo a la serie de los números primos, algo así como «un, dos, tres,... ¡ya!». No funciona; los números primos no aparecen cada tres naturales compuestos. Vamos a probar otra cosa: «Un, dos, tres, veinte, cien,... ¡ya!». Tampoco funciona. Y así, podríamos seguir probando *ad infinitum*. A día de hoy todavía no se sabe si esta «banda» de números lleva un ritmo endiabladamente complicado o es que simplemente carece por completo del sentido del ritmo.

¿Cómo se hace para imponer una métrica a una sucesión de números? Hay muchas formas de hacerlo. Lo importante es que cuando se consigue se debe ser capaz de predecir cuál es el número siguiente a uno dado. Por ejemplo, la sucesión

2, 4, 6, 8,...

no plantea problema, pues cualquiera puede saber que el siguiente número es el 10.

En el caso de

1, 3, 5, 7,...

también es sencillo adivinar que el número siguiente es el 9. La primera es la sucesión de los números pares, y la segunda, la de los impares. Otro ejemplo:

2, 3, 5, 9, 17,...

Aquí cada número se obtiene multiplicando el anterior por 2 y restando 1 al resultado.

Este tipo de series se utilizan muchas veces como pasatiempo y también forman parte del contenido de algunos testes de inteligencia.

En matemáticas, el asunto está resuelto cuando obtenemos lo que se llama «expresión del término general» a_n, que es una expresión que nos da el valor de cada término sin más que dar valores a n.

Por ejemplo, en la sucesión de números pares tendríamos que

$$a_n = 2n$$

Si $n = 1$ $a_1 = 2 \times 1 = 2$;

Si $n = 2$ $a_2 = 2 \times 2 = 4$;

Si $n = 3$ $a_3 = 2 \times 3 = 6$.

En el caso de la sucesión de números impares tendríamos que el término general viene dado por

$$a_n = 2n + 1$$

Mediante este sistema podemos conocer el valor de un término cualquiera. Si deseamos saber cuánto vale el término que ocupa el lugar 27 no tenemos más que hacer $n = 27$ en la expresión del término general:

$$a_{27} = 2 \times 27 + 1 = 55.$$

Encontrar la fórmula del término general es tanto como haber descubierto la ley de formación de la sucesión. La cuestión entonces es la siguiente: si conocemos la expresión del término general, conocemos la ley de formación, y obtener términos cualesquiera de la sucesión no plantea mayores problemas. Sin embargo, cuando la cuestión se plantea al revés, el problema puede llegar a ser tan complicado como se quiera. Por ejemplo, la sucesión de números

$$\frac{2}{4}, \frac{5}{7}, \frac{10}{12}$$

puede no resultar tan sencilla de predecir, y es que el término general de esta sucesión es

$$a_n = \frac{n^2 + 1}{n^2 + 3}$$

Para hallar los tres primeros términos no tenemos más que dar valores a n:

$$a_1 = \frac{1^2 + 1}{1^2 + 3} = \frac{2}{4}$$
$$a_2 = \frac{2^2 + 1}{2^2 + 3} = \frac{5}{7}$$
$$a_3 = \frac{3^2 + 1}{3^2 + 3} = \frac{10}{12}$$

Pues bien, ésta es una gran parte del esfuerzo que los matemáticos han dedicado a lo largo de la historia al estudio de los números primos. Un intento de que respondieran a algún tipo de pauta y que ha llevado a frustraciones y fracasos de toda índole. Porque ¿es posible que esta caótica colección de números sólo se rija por las leyes del azar? De todas maneras, en matemáticas se debe matizar cuando se habla de fracasos, ya que, si los estudiosos «fracasan» puede que en sus investigaciones no hayan llegado a alcanzar los objetivos propuestos, pero en su andadura han trazado nuevos caminos, han inventado otras formas de hacer matemáticas y han abierto las puertas a nuevos paradigmas. Muchas veces parece como si el objetivo buscado no fuera más que una excusa para plantearse nuevos problemas. En este sentido, los números primos han sido y siguen siendo una de las fuentes más fructíferas de paradojas y conjeturas.

5. Primos gemelos

Si no es posible establecer una ley general de formación, por lo menos se puede intentar estudiar el comportamiento de algunos números primos que posean características especiales. Es como estar delante de una ventana por la que van pasando un interminable conjunto de personas diferentes. Sabemos que unas son hombres y otras mujeres, pero no conseguimos establecer ninguna pauta que nos permita predecir cuál será el momento en que pasará una u otra. Pero, de repente, un día nos fijamos en alguna característica especial, nos damos cuenta de que, de vez en cuando, pasan hombres con sombrero, personas con gafas de sol y otras con paraguas. Intentamos entonces encontrar alguna regla que defina la aparición de grupos concretos. Observar, por ejemplo, si los del sombrero aparecen cada cien veces que pasa una mujer, o bien que cada vez que pasa uno después siempre pasa

una mujer. Cualquier cosa que nos permita determinar una pauta. Puede ser que la encontremos y que la cosa funcione, pero que empiece a fallar cuando contabilicemos el paso de tres millones de personas. Entonces exclamaremos: ¡Oh! ¡Casi! Este «casi» nos llevará a decir que «las cosas funcionan como si…», expresión que ha sido muy frecuente en la historia de los números primos.

Es cierto que se ha conseguido caracterizar a algunas familias de números primos (de hecho hay algunas docenas) que han permitido ciertos avances a lo largo de la historia. Por el momento, vamos a fijarnos en unas singulares parejas de números primos cuyas características nos ayudarán a comprender un poco mejor las dificultades matemáticas que plantean estos erráticos números.

La soledad de los números primos

Los números primos pueden estar separados por millones y millones de números o bien por uno solo, que es lo más juntos que pueden estar; en cualquier caso, jamás se tocan, salvo el 2 y el 3. Este hecho ha servido de metáfora para dar título a un clásico de la literatura reciente, La soledad de los números primos, de Paolo Giordano. En uno de los párrafos de la novela se pone de manifiesto la metáfora de forma explícita: «En una clase de primer curso Mattia había estudiado que entre los números primos hay algunos aún más especiales. Los matemáticos los llaman números primos gemelos: son parejas de números primos que están juntos, o mejor dicho, casi juntos, pues entre ellos media siempre un número par que los impide tocarse de verdad. Números como el 11 y el 13, el 17 y el 19, o el 41 y el 43. Mattia pensaba». que Alice y él eran así, dos primos gemelos, solos y perdidos, juntos pero no lo bastante para tocarse de verdad.

Dos números primos no pueden ser consecutivos, ya que todo número primo es impar y el número siguiente forzosamente ha de ser par, por lo que no podría ser primo. Por lo tanto, lo más juntos que pueden estar dos números primos es separados por dos unidades. La excepción la constituyen el 2 y el 3, que son consecutivos; además, el 2 es el único primo par.

Entre los cien primeros números naturales encontramos las siguientes parejas separadas por dos unidades: (3,5) (5,7) (11,13) (17,19) (29,31) (41,43) (59,61) y (71,73).

A estas parejas se las llama «primos gemelos» o, simplemente, «gemelos».

Los gemelos responden a la estructura (p, $p + 2$) donde p es un número primo.

Ésta es la lista de todos los primos gemelos que existen entre los mil primeros números:

(3, 5)	(5, 7)	(11, 13)	(17, 19)	(29, 31)
(41, 43)	(59, 61)	(71, 73)	(101, 103)	(107, 109)
(135, 139)	(149, 151)	(179, 181)	(191, 193)	(197, 199)
(227, 229)	(239, 241)	(269, 271)	(281, 283)	(311, 313)
(347, 349)	(419, 421)	(431, 433)	(461, 463)	(521, 523)
(569, 571)	(599, 601)	(617, 619)	(641, 643)	(659, 661)
(809, 811)	(821, 823)	(827, 829)	(857, 859)	(881, 883)

Sabemos que los primos gemelos empiezan a escasear conforme se avanza en la serie de los números naturales. Sin embargo, se tiene constancia, gracias a métodos computacionales, que sigue habiendo primos de esta clase entre números extraordinariamente grandes, lo que ha llevado a los matemáticos a conjeturar que existen infinitos números primos gemelos, conjetura que a día de hoy nadie ha conseguido demostrar.

Otro grupo de números primos que llama la atención cuando observamos la tabla de los contenidos entre los cien primeros números naturales es el formado por los números 3, 5 y 7.

Siendo p un número primo, estos tres números responden a la estructura (p, $p + 2$, $p + 4$). Es un grupo que podría llamarse «trillizos», pero que se denomina «triplete». En realidad, no haría falta llamarlos de ninguna manera, ya que no existen más que estos tres. Éste sí es un resultado corroborado. Por suerte un tema cerrado, ya que de otra forma, los tripletes habrían dado lugar a otra colección de conjeturas que todavía estarían sin resolver.

Los primos gemelos más grandes que se conocen (hasta agosto de 2009) son los formados por los números

$$65.516.468.355 \times 2^{333333} - 1 \text{ y } 65.516.468.355 \times 2^{333333} + 1,$$

que tienen la friolera de cien mil trescientas cincuenta y cinco cifras.

Separaciones infinitas

Los números primos gemelos han dado lugar a varias conjeturas, además de la que afirma que son infinitos. Una de ellas, de carácter más general, fue establecida en 1849 por el matemático francés Alphonse de Polignac (1817-1890), según la cual para cada C existen infinitos pares de números primos que están separados por 2 x C números compuestos. Es decir, que existen infinitos números primos separados por cuatro números compuestos, por seis números compuestos, por ocho números compuestos y así sucesivamente. En el caso en que C = 1 se tiene la conjetura de los primos gemelos.

6. Magia y matemáticas

Hemos recalcado la importancia que tienen y han tenido los centros de información a lo largo de la historia. Ahora debemos hacer hincapié en un segundo aspecto que adquiere cierta importancia cuando se recorre la historia de las matemáticas, especialmente si se hace de la mano de los números. Se trata de la posible relación que ha podido existir entre la magia y las matemáticas. Al hablar de magia nos referimos a una parte de la tradición histórica de las matemáticas a la que se suele llamar «aritmología». Existe una relación entre las matemáticas y la aritmología similar a la que ha existido entre la astronomía y la astrología o entre la química y la alquimia. En la actualidad, estas parejas han quedado prácticamente disociadas, pero a lo largo de la historia han formado matrimonios de conveniencia que no se pueden soslayar si se quiere tener una perspectiva histórica de lo que ha supuesto una determinada «visión del mundo» en cada etapa del desarrollo de la ciencia.

Los números y, por consiguiente, los números primos, han sido objeto no sólo de investigación matemática, sino también de investigación filosófica y, sobre todo, de culto religioso. Cuando entran a formar parte del entramado cultural lo hacen bajo formas muy distintas: los encontraremos la concepción filosófica de la escuela pitagórica, en la que las figuras geométricas y los números son el principio de todas las cosas.

Nos vamos a encontrar, pues, con misterios y leyendas que rodean a matemáticos célebres, como Mersenne o Fermat, de quienes se habla de la posibilidad de que conocieran métodos matemáticos de gran sencillez que les permitieran alcanzar metas que a otros les estaban vedadas. El historiador Libri afirmaba que «Fermat sabía cosas que nosotros ignoramos, y para llegar a él se precisan métodos más perfectos que los inventados después». No hay que olvidar que Fermat, a diferencia de otros muchos matemáticos de su época, no era del tipo de científicos que encubrían sistemáticamente sus conocimientos, aunque sí podría haber ocultado la manera de llegar a ellos.

Vamos a adentrarnos en épocas en las que el rigor matemático, tal y como empezaría a concebirse en el siglo XVIII, no tenía la importancia que le damos ahora. Se trataba de crear un edificio matemático con un carácter de índole más práctica que teórica. En este aspecto, la enseñanza tradicional, con todo lo que podía conllevar de simbología mística, no suponía un impedimento, sino más bien todo lo contrario, era un espacio en el que se podía hacer volar la imaginación.

En este sentido, tenemos una idea muy equivocada de lo que son las matemáticas, porque tenemos una idea también equivocada de lo que son los matemáticos y en qué consiste su trabajo. El desconocimiento del quehacer matemático no sólo genera desconocimiento sobre la naturaleza de la mente matemática, sino que en parte también ha sido fuente de su impopularidad. El resultado final de una investigación, que suele tener formato de teorema, ha sido ordenado, revisado y pulido de tal forma que adolece casi siempre de un cierto hermetismo para el que carece de una preparación previa. Es difícil, pues, hacer comprender a alguien la belleza que se puede encerrar en enunciados tan técnicos y de tan extrema pulcritud lógica. Sin embargo, la tarea del investigador matemático no se desarrolla

en ese esquema, más bien se mueve en una intrincada selva en la que no se vislumbran apenas caminos y en la que, además, es noche oscura.

Los números en el Pentateuco

Números es el cuarto libro de la Biblia, forma parte del Pentateuco y se atribuye a Moisés. En una visión superficial, Números es un libro de contabilidad y, en ese sentido, tiene un indudable valor histórico, ya que da cabal cuenta de todas las cantidades presentes, desde jefes de las tribus hasta cabezas de ganado, que conformaban el escenario histórico al que hace referencia. Pero también es un libro de claves secretas para aquellos iniciados que saben descifrar sus mensajes, pues los números no sólo representan cantidades, sino que también tienen un significado. Por ejemplo, el 1 simboliza a Dios, el 2 al hombre, el 3 a la totalidad de las cosas, etc. Es curioso que el número 5 represente una cantidad indefinida, «unos cuantos». Por ejemplo, en la multiplicación de los panes se dice que Jesús tomó cinco panes, es decir, «algunos» panes. La curiosidad reside en el hecho de que 5 es el primer número de objetos que no podemos contabilizar con un golpe de vista. Se sabe que podemos contar, sin hacer operaciones, colecciones de hasta cuatro objetos; a partir de esa cantidad estamos obligados a repartir en grupos y sumar.



El Pentateuco es uno de los cinco primeros libros de la Biblia.

El hecho de que la mente matemática se adentre por las sendas más recónditas del espíritu ha llegado incluso a inquietar a los guardianes del orden moral. Una buena prueba de ello son las palabras de san Agustín al respecto: «El buen cristiano debe estar alerta en contra de los matemáticos y de todos quienes hacen profecías vacuas. Existe el peligro de que los matemáticos tengan pacto con el demonio y la misión de ofuscar el espíritu del hombre para confinarlo en los linderos del infierno».

Existe un tercer punto que, junto a lo que hemos llamado centros de información y a los aspectos mágicos de los números, hay que tener en consideración para comprender la larga andadura de los números primos a través de la historia. Se trata de las cualidades excepcionales para los números de que han sido dotadas algunas personas. Cualidades que la mayoría de las veces han ido parejas con las letras. La mayoría de los matemáticos ilustres que veremos «rondando» a los números primos poseían también dotes extraordinarias para las lenguas, lo que en el fondo no es de extrañar, pues como hemos explicado al comienzo del libro, los números y las letras están emparejados en cuanto a su naturaleza abstracta. En épocas en las que las herramientas de cálculo eran prácticamente inexistentes, la capacidad de cálculo mental era imprescindible. Una capacidad que va más allá del mero cálculo numérico, más propio del mundo del espectáculo que de la matemática. Hombres de la talla de Fermat, Mersenne, Euler o Ramanujan poseían el don mágico de «ver» en el universo de los números. Esa capacidad les permitía descubrir relaciones que se les aparecían a ellos y no a otras personas; relaciones que requerían de demostraciones que muchas veces quedaban fuera de su alcance y en algunos casos hasta fuera de sus intereses personales.

Los calculistas

Los calculistas profesionales aparecieron en el siglo XIX. Empezaron a «ponerse de moda» y a ofrecer espectáculos en los escenarios de los teatros de Europa y América, a los que acudía puntualmente un público devoto de tan prodigiosas proezas mentales. Zerah Colburn, el primero de los calculistas profesionales del que se posee una amplia documentación,

nació en Cabot, Vermont (EE UU) en 1804.

En una ocasión le pidieron que calculara el producto de 21.734 por 543. Casi al instante respondió 11.801.562. Alguien de su concurrida audiencia le preguntó cómo Jo había hecho: «He visto que 543 es igual a tres veces 181. Entonces he multiplicado primero 21.734 por tres y luego el resultado por 181», contestó satisfecho Colburn, que normalmente se retrasaba algún segundo cuando debía multiplicar números de cinco cifras. Todo esto sucedía en 1812 y Zerah Colburn tenía entonces ocho años.

Capítulo 3
Los nuevos paradigmas

Contenido:

1. *Marín Mersenne*
2. *Pierre de Fermat*
3. *Leonhard Euler*
4. *La conjetura de Goldbach*

A mediados del siglo XVII estaba naciendo un movimiento científico importante, pero a extramuros de las instituciones académicas. Por entonces ya habían hecho su aparición las primeras universidades europeas, centros en los que se atesoraba conocimiento, pero que se articulaban con una rigidez interna impermeable a los nuevos paradigmas. Esto planteaba un serio problema para todos aquellos que quisieran proseguir el curso de sus investigaciones al margen del círculo académico, ya que fuera de él no podían percibir ningún tipo de honorarios. Empezó así la época de los grandes mecenazgos: nobles y terratenientes poderosos tenían a gala acoger en su seno a mentes privilegiadas que empezaban a abrir las puertas a una nueva concepción del mundo. En la mayoría de las biografías aparecen, junto a los nombres célebres de los grandes científicos, los de sus mecenas. Pero esto planteaba, una vez más, un problema de comunicación.

Nació entonces un centro muy especial por el importantísimo papel que desempeñó en la comunicación científica de la época. Ese peculiar centro, que sería la simiente de la futura Académie des Sciences (fundada por Colbert en 1666), se encontraba en la celda de un convento de París, y el hombre que lo había creado y que lo mantenía vivo era el padre Mersenne.

1. Marín Mersenne

Mersenne nació el 8 de septiembre de 1588 en Oizé, en el actual departamento de Sarthe (Francia). De sus andanzas en los primeros años de su vida apenas se tienen datos. Se sabe que en 1604 ingresó como interno en la Fleche, un colegio fundado en 1603 por Enrique IV y dirigido por la orden de los jesuitas, donde permaneció un

año; durante ese periodo trabó una sólida amistad con Descartes, condiscípulo suyo y con quien mantendría una relación de amistad toda su vida.
En 1609 inició sus estudios de teología en La Sorbona, donde se licenció dos años después, para ingresar en la Orden de los Mínimos. En 1612 fue nombrado presbítero del convento de la Anunciación, en París.



Marín Mersenne (1588-1648)

Desde 1614 a 1618 estuvo impartiendo clases de filosofía en el convento de Nevers. Luego volvió a su celda de París, donde permanecería hasta su muerte, acaecida el 1 de septiembre de 1648. Con el ánimo de servir hasta el final a los objetivos de la ciencia, Mersenne dejó escrita en su testamento la voluntad póstuma de que su cuerpo fuera donado a la facultad de Medicina para estudios anatómicos.
Entre las primeras obras de Mersenne, que fueron de carácter puramente teológico, figuran *Quaestiones celeberrimae in Genesim* (1623), *La verdad de las ciencias contra los escépticos y los pirrónicos* (1625) y *Cuestiones teológicas, físicas, morales y matemáticas* (1634). Entre sus obras científicas hay que destacar

Armonía universal (1636), en la que estableció una fórmula que relacionaba la longitud de una cuerda y la frecuencia del sonido emitido por ésta.

Dicha fórmula le permitió crear una escala donde todos los intervalos fueran iguales, lo cual haría innecesaria la famosa coma pitagórica, estableciendo las bases teóricas para la que habría de ser una de las mayores revoluciones de la historia de la música: la escala cromática o temperada.

La orden de los Mínimos

El nombre de esta orden responde al hecho de que todos sus miembros debían acatar unos mínimos principios religiosos. Su objetivo era huir de cualquier cuerpo doctrinal que en función de un conjunto de verdades reveladas acabara imponiendo pautas de conducta excesivamente restrictivas. De hecho, lo único que combatían sin ambigüedades era el ateísmo. Se dedicaban fundamentalmente a la oración, el estudio y la enseñanza, y procuraban por todos los medios que sus convicciones religiosas no interfirieran nunca ni en la educación ni en el desarrollo científico. Buena prueba de ello, es la encarnizada defensa que Mersenne hizo de la figura y el pensamiento de Galileo.

Los números de Mersenne

La gran obra científica de Mersenne de carácter puramente matemático fue *Cogitata Physico-Mathematica* (1644), en la que aparece su célebre estudio sobre los números primos. En el prólogo de la misma Mersenne afirma que de entre todos los primos que hay entre 2 y 257, el número$2^p - 1$ sólo es primo si el valor de p es alguno de los siguientes números:

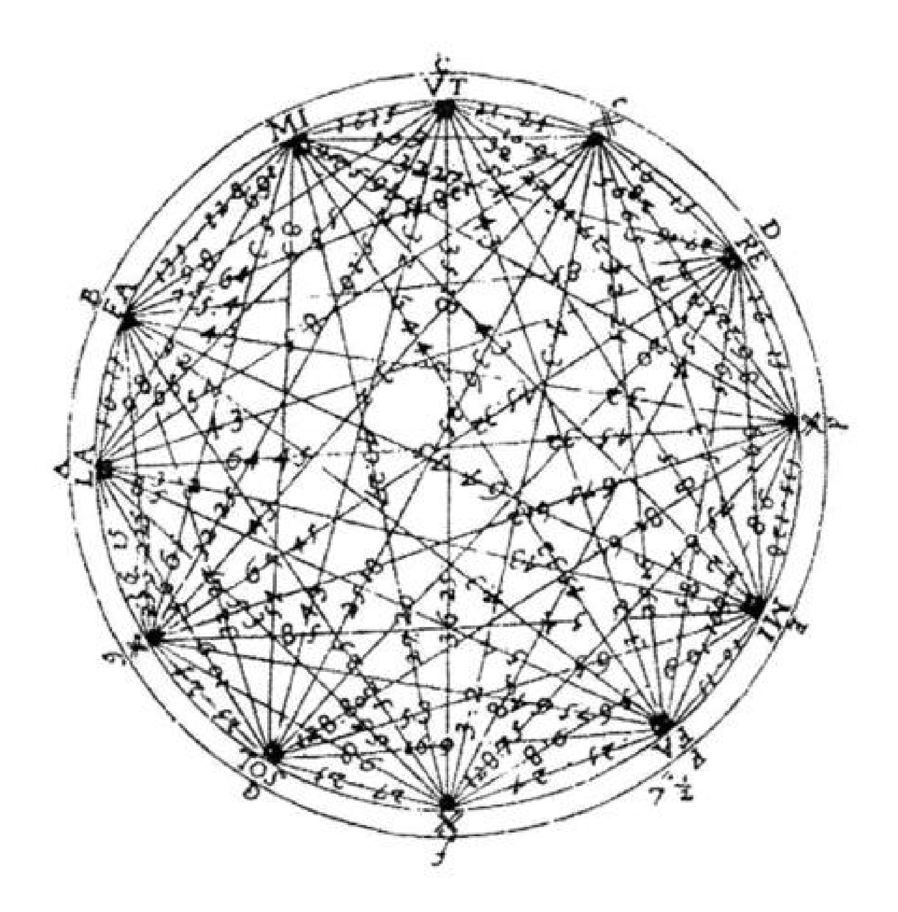
2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.

Cuando tomamos 2 y lo elevamos al último número de la lista, el resultado es un número de setenta y siete cifras. Cómo se las arregló Mersenne con los medios de cálculo de la época para decidir que éste era un número primo constituye un auténtico misterio que nadie ha conseguido resolver.

Es fácil demostrar que si $2^p - 1$ es primo, entonces p debe ser primo (o lo que es lo mismo, que si p no es primo, entonces tampoco lo es $2^p - 1$). Este resultado, que ya era conocido en la época de Mersenne, lo llevó a investigar qué sucedía cuando en esta expresión se introducía un número *p* que fuera primo. También se sabía que $2^p - 1$ era primo para los valores $p = 2, 3, 5, 7, 13, 17$ y 19, pero no para $p = 11$. Tuvieron que pasar cien años para que Euler consiguiera demostrar que $2^{31} - 1$ era primo. En 1947 se resolvió completamente la lista, quedando del siguiente modo,

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 \text{ y } 127,$$

de manera que en la lista original sobraban dos números y faltaban tres. A pesar de todo, a estos números se los sigue llamando «números de Mersenne», números que actualmente desempeñan un importante papel en los llamados «tests de primalidad», un conjunto de algoritmos encaminados a decidir si un número es o no primo.



Mersenne estudió las vibraciones de las cuerdas y creó una escala dividida en doce intervalos iguales.

Centro neurálgico

La pequeña celda en la que Mersenne pasó los últimos treinta años de su vida, en el convento de los Mínimos, junto a la Place Royal, acabó convirtiéndose en el centro neurálgico de la ciencia europea de su tiempo. Se llegó a decir que informar a Mersenne de un descubrimiento era tanto como difundir una publicación por toda Europa. Después de su muerte se encontraron en su celda documentos que atestiguaban que Mersenne mantenía setenta y ocho líneas diferentes de correspondencia, en otras tantas líneas de investigación, en las que figuraban personalidades del mundo científico de entonces con nombres tan relevantes como Torricelli, Descartes, Pascal, Gassendi, Roberval, Beaugrand o Fermat.

2. Pierre de Fermat

Fermat (1601-1665) ha llegado a ser una auténtica leyenda en el mundo de las matemáticas. Sus descubrimientos, especialmente en la teoría de números, rama de la que se le puede considerar fundador, lo han hecho pasar a la historia de las matemáticas como el «príncipe de los aficionados». Además, poseía un dominio absoluto de las lenguas clásicas, latín y griego, así como de la mayoría de las lenguas europeas que se hablaban entonces.

Fermat gozaba de una posición privilegiada que le permitía dedicarse plenamente a su pasión por los números. Había nacido en una familia acomodada y sus estudios de legislatura le permitieron ocupar un cargo de funcionario en la Consejería Real del Parlamento local de Toulouse. Una de las exigencias de este cargo público era que debía mantenerse alejado de todo tipo de actividades sociales con el ánimo de evitar cualquier asomo de corrupción. Se casó con Louise de Long, una prima de su madre, con la que tuvo tres hijos: el mayor, Climent-Samuel, sería quien se encargaría de publicar su obra, mientras que sus dos hijas acabaron siendo monjas en un convento.

Fermat ni siquiera viajaba; el único desplazamiento destacable lo llevó a París, donde, por mediación de Pierre de Carcavi (1600-1684), un influyente matemático francés, entró en contacto con el padre Mersenne en el convento de los Mínimos.

Hay gente aficionada al cultivo de las flores que dedica gran tiempo a conseguir que germinen especies nuevas, bien de semillas procedentes de lejanos países o por cruces que en ocasiones reportan agradables sorpresas. Fermat cultivaba números. Una mañana se asomaba a su jardín mental y se encontraba con una nueva especie que, para el resto de los mortales, había hecho su aparición de forma casi milagrosa. No formaba parte de aquellos matemáticos que ocultan sus resultados, pues se los ofrecía a todo el mundo, pero casi nunca explicaba cómo los había obtenido. La propiedad «todo número primo de la forma 4n + 1 es suma de dos cuadrados» fue, por ejemplo, uno de los muchos resultados que nunca demostró y que fue probado por Euler en 1749 después de haber trabajado durante siete años en la demostración. Gauss consideraba este resultado como «una de las más bellas flores que Fermat había descubierto en su jardín de los números».

El pequeño teorema de Fermat

En el año 1995 Andrew Wiles hizo que Fermat ocupara un espacio en las primeras páginas de los periódicos después de que consiguiera demostrar una de las más famosas conjeturas de la historia: Si n es un número entero mayor que 2 (o sea, $n > 2$), entonces no existen números enteros x, y, z distintos de O tales que cumplan la igualdad

$$x^n + y^n = z^n,$$

conjetura que es conocida como el «último teorema de Fermat».

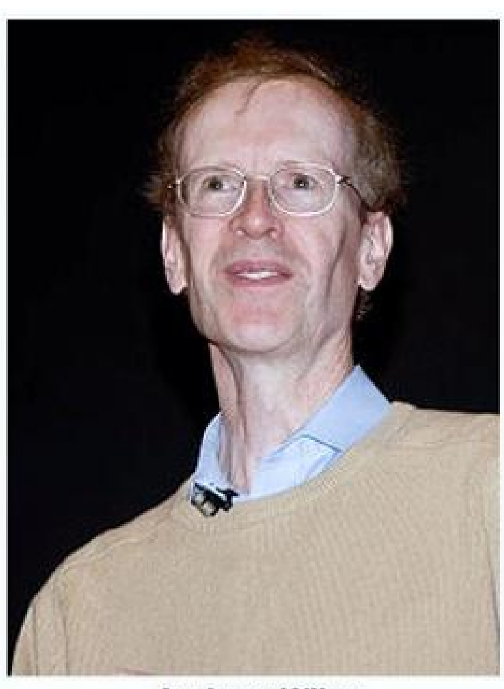
Pero hay otro teorema, mucho menos popular, que es conocido como pequeño teorema de Fermat, que ha llegado a tener una gran relevancia en la teoría de los números primos.

Su enunciado apareció por primera vez en una carta que Fermat envió el 18 de octubre de 1640 a Bernard Frénicle de Bessy (1605-1675), amigo y también

matemático aficionado con quien Fermat compartía algunos de sus resultados (ambos formaban parte del selecto círculo de Mersenne). La misiva decía así:

«Todo número primo mide una de las potencias menos uno de cualquier progresión en la que el exponente es un múltiplo del primo dado menos uno. (...) Y esta proposición es generalmente cierta para todas las progresiones y todos los números primos; le enviaría la prueba si no temiese que es demasiado larga».





El conocido como último teorema de Fermat fue resuelto en 1995 por el británico Andrew John Wiles. Dos años antes, el matemático británico presentó una primera demostración, en la que, sin embargo, se reveló un error que posteriormente fue capaz de corregir.

Como era habitual en él, Fermat omite la demostración, aduciendo, como en el caso de su célebre último teorema, que es demasiado larga. Es muy probable, y la mayoría de los historiadores actuales coinciden con ello, que no conociera realmente la demostración de ésta y otras conjeturas a las que llegaba. De todas maneras, Fermat se consideraba a sí mismo un «aficionado», lo que le permitía tomarse ciertas licencias.

El enunciado que figura en la carta enviada a Bessy resulta un tanto críptico, por lo que aquí se expresa siguiendo la terminología moderna.

Se dice que dos números son primos entre sí (o coprimos) cuando son primos relativos, es decir, no tienen factores en común. Por ejemplo, 8 y 27 son primos entre sí, ya que no tienen factores en común: $8 = 2^3$ y $27 = 3^3$. En cambio, 12 y 15 no lo son, ya que tienen el número 3 como factor común: 12 = 3 x 4 y 15 = 3 x 5.

El teorema afirma entonces que si *p* es un número primo y a otro número cualquiera, de manera que *a* y *p* sean primos entre sí, entonces se cumple que $a^p - a$ es divisible por *p*.

Por ejemplo, tomemos el número primo 3 y el número 8 que es primo con éste, entonces $8^3 - 8 = 512 - 8 = 504$ es divisible entre 3. En efecto, comprobamos que 504/3 = 168.

Se puede afirmar que el pequeño teorema de Fermat es pequeño, pero matón (el adjetivo de pequeño fue utilizado por primera vez en 1913 por el matemático alemán Kurt Hensel), ya que es uno de los teoremas a los que más se recurre cuando se trata de implementar un test de primalidad para decidir si un número muy grande es o no primo. De hecho, el mismo Fermat debió de utilizarlo como herramienta matemática para descomponer algunos números primos grandes en producto de factores. Se sabe, por ejemplo, que fue capaz de encontrar 100.895.598.169 como producto de los números 898.423 y 112.303, ambos primos, en respuesta a una petición de Mersenne, que quería saber si dicho número era primo. Aún así, se hace difícil saber cómo Fermat podía manejarse con números tan grandes.

El teorema fue demostrado por primera vez por Euler en 1736 (Leibniz tenía una demostración similar, pero nunca llegó a publicarla). Asimismo, Gauss hizo otra demostración en su famoso libro *Disquisitiones Arithmeticæ*, publicado en 1801. El mismo Euler haría posteriormente dos demostraciones más. De todas ellas, la más sencilla es la primera de Euler y puede entenderse con conocimientos básicos de matemáticas (véase los anexos).

Recalquemos que el pequeño teorema de Fermat constituye un método para saber si un número no es primo sin necesidad de encontrar ninguno de sus factores. Veamos un ejemplo sencillo:

Supongamos que $p = 9$ y $a = 2$; se tiene entonces que $2^9 - 2 = 510$, que no es divisible por 9, de lo que se concluye que 9 no es primo, cosa que ya sabíamos. La aportación del método consiste en la posibilidad de aplicarlo a números muy grandes.

Hay que prestar atención al hecho de que el pequeño teorema de Fermat plantea una condición necesaria, pero no suficiente; esto significa que si p es primo se cumple necesariamente la condición, pero el hecho de que se cumpla no quiere decir que p sea primo. Por ejemplo, si tomamos $p = 10$ y $a = 3$, se tiene que

$$3^{10} - 3 = 59.046,$$

que no es primo, ya que es divisible por 3.

La versión china

Existen fuentes documentadas (J. Needham) que especulan con la posibilidad de que los matemáticos chinos ya hubieran establecido, dos mil años antes que Fermat, una hipótesis, conocida como la «hipótesis china», con un resultado muy similar al que se obtiene con el pequeño teorema de Fermat.

Dicha hipótesis afirma que p *es un número primo si y sólo si* $2^p - 2$ *es divisible por p. Hasta aquí la hipótesis china se puede considerar como un caso especial del pequeño teorema de Fermat. Sin embargo, el recíproco, que asegura que si se cumple la condición entonces* p *es primo, no es cierta, por lo que la hipótesis china debe ser considerada falsa.*

Los números de Fermat

Un «número de Fermat» es un número natural que tiene el siguiente aspecto:

$$2^{2n} + 1$$

Se suele simbolizar con la letra F (de Fermat) con un subíndice *(n)* que indica el número del que se trata, de manera que F_0 es el primer número de Fermat, F_1 el segundo y así sucesivamente.

Vamos a calcular el valor de los cinco primeros números de Fermat. Recordemos que cualquier número elevado a 0 vale 1, de manera que

$$2^0 = 1;\ 2^1 = 2;\ 2^2 = 4;\ 2^3 = 8$$

Sustituyendo en la fórmula anterior tendremos que:

$$F_0 = 2^{20} + 1 = 2^1 + 1 = 3$$
$$F_1 = 2^{21} + 1 = 2^2 + 1 = 4 + 1 = 5$$
$$F_2 = 2^{22} + 1 = 2^4 + 1 = 16 + 1 = 17$$
$$F_3 = 2^{23} + 1 = 2^8 + 1 = 256 + 1 = 257$$
$$F_4 = 2^{24} + 1 = 2^{16} + 1 = 65.536 + 1 = 65.537$$

Fermat conjeturó que todos los números que se obtenían de esta forma eran primos. Los cinco primeros, 3, 5, 17, 257 y 65.537, lo son.

Cuando *n* vale 5, el número que se obtiene es:

$$F_5 = 2^{25} + 1 = 2^{32} + 1 = 4.294.967.296 + 1 = 4.294.967.297.$$

Fermat no tenía entonces recursos para saber si un número superior a los cuatro mil millones era o no primo. Pero, al parecer, Euler sí, y en 1732 encontró una factorización de este número como producto de otros dos:

$$4.294.967.297 = 641 \times 6.700.417.$$

Euler había «cazado» a Fermat en una falsa conjetura. Era la primera vez que sucedía algo así. A pesar de que la conjetura fuera falsa, los números de Fermat han dado mucho de sí, no sólo porque han generado, cómo no, nuevas preguntas y

conjeturas, sino porque también han resultado ser útiles a la hora de confeccionar un test de primalidad.

De momento se sabe que sólo los cinco primeros números de Fermat son primos, lo que no quiere decir que no haya más, incluso que pueda haber infinitos. La factorización completa sólo se conoce hasta $n = 11$. Y es que factorizar un número como producto de primos no es tarea fácil.

Como veremos más adelante, en esta dificultad se basa uno de los sistemas de encriptación más populares de los que se emplean actualmente.

3. Leonhard Euler

No hay rama de la matemática clásica, desde el cálculo, las ecuaciones diferenciales, la geometría analítica y diferencial, pasando por la teoría de números o las series y el cálculo de variaciones, en la que no aparezca el nombre del matemático y físico suizo Leonhard Euler (1707-1783). Se trata de uno de los matemáticos más prolíficos de todos los tiempos: después de su muerte, acaecida en San Petersburgo, continuaron apareciendo escritos suyos que fueron publicados año tras año por la Academia de Ciencias de San Petersburgo. Todavía han de publicarse, bajo los auspicios de la Academia de Ciencias de Suiza, sus obras completas, que se estima que ocupen cerca de noventa grandes volúmenes.

Euler mostró siempre un especial interés por los números primos: construyó tablas para todos los comprendidos entre 1 y 100.000, para lo cual creó fórmulas que le permitían obtener una cantidad asombrosa de ellos. Una de las más interesantes fue

$$x^2 + x + q$$

que proporcionaba números primos para valores de x siempre que fueran mayores que 0 y menores que $q - 2$. Todo esto lo hizo dando valores $q = 2, 3, 5, 11$ y 17. Se trataba de matemáticas experimentales, cuyo objetivo era conseguir resultados prácticos, por lo que muchos de ellos carecían de demostraciones rigurosas. Sin embargo, Euler, a diferencia de Fermat, no ocultaba ninguna demostración: si la tenía, la publicaba, y si no lo hacía es porque carecía de ella.

Euler estableció un cambio en el panorama matemático, un escenario que era consecuencia de un lento pero continuo cambio en el paradigma. Entre sus muchas aportaciones destacan tres que tuvieron una importancia decisiva en las investigaciones posteriores en torno a los números primos: el concepto de función, las sumas infinitas y la utilización de cantidades imaginarias (a esta última nos referiremos más adelante).



Billete de banco suizo de diez francos del año 1997 y que reproduce, en el anverso, un retrato de Euler, mientras que en el reverso se observa una turbina hidráulica, el Sistema Solar y la propagación de la luz a través de varias lentes. Todo ello alude a la contribución de Euler a la física matemática.

Las funciones

Euler estableció de manera clara los fundamentos de lo que siglos más tarde se conocería como «análisis matemático». A él se debe la notación que utilizamos actualmente para simbolizar una función $f(x)$. Una función actúa como una máquina que transforma números en otros números según una pauta establecida (nos estamos refiriendo exclusivamente a funciones reales de variable real). Por ejemplo, si la pauta dice que al número en cuestión se le debe sumar una cantidad fija como, por ejemplo, 3, la función se escribe de la siguiente manera:

$$f(x) = x + 3$$

A partir de ese momento la pauta ya puede utilizarse:

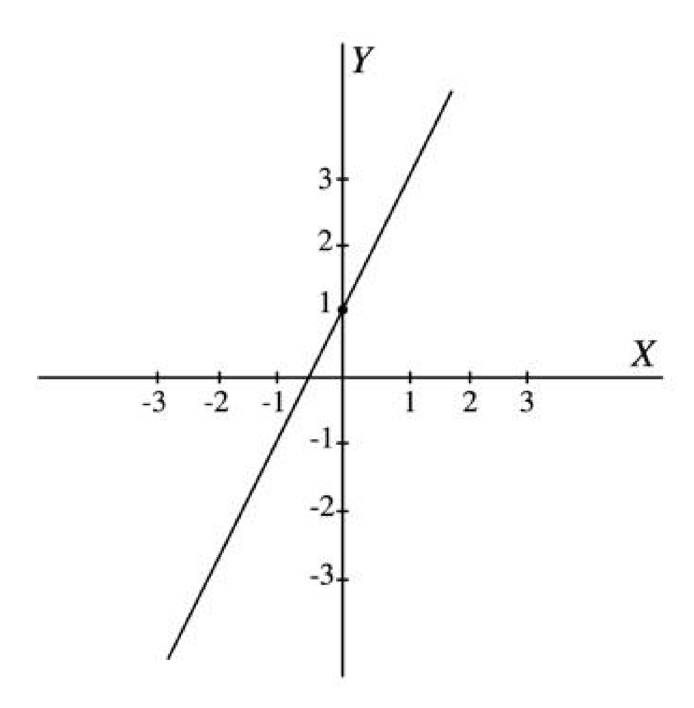
$$f(1) = 1 + 3 = 4$$
$$f(2) = 2 + 3 = 5$$
$$f(24) = 24 + 3 = 27$$
$$f(0{,}32) = 0{,}32 + 3 = 3{,}32$$

Una función real de variable real asigna a cada número real otro número real. Por ejemplo, la función $f(x) = 2x + 1$ asigna a cada valor de x el doble de dicho valor más uno. Una simple tabla de valores como ésta:

$$g(x) = 2x + 1$$

x	1	2	3	-1	-2	-3
g(x)	3	5	7	-1	-3	-5

... nos permitiría dibujar la gráfica siguiente de la función por puntos.



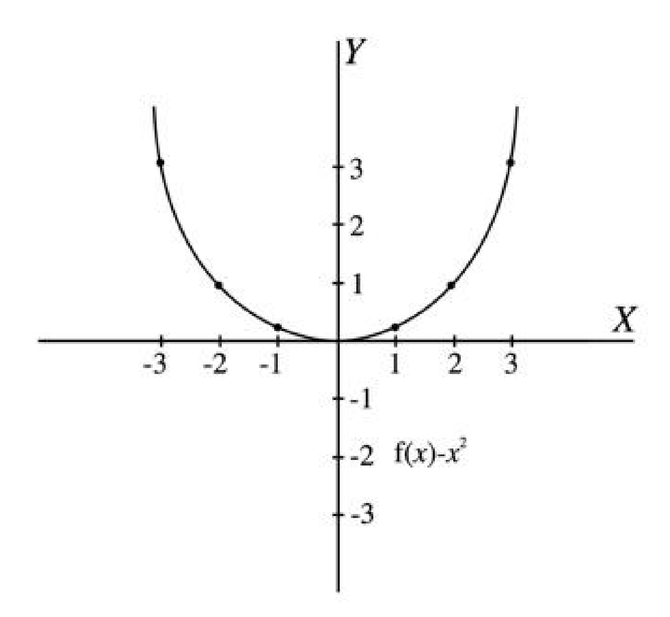
En este caso, la representación es muy sencilla porque se trata de una recta, y para dibujarla basta con dos puntos.

Sin embargo, una función como $f(x) = x^2$, que tendría una tabla como la siguiente:

$f(x) = x^2$

x	1	2	3	4	...
x^2	1	4	9	16	...

... no es tan sencilla de dibujar:



Es cierto que cuantos más puntos tengamos más precisa será la gráfica, pero cuando la expresión deja de ser lineal, es decir, en el momento en que la variable, la x, aparece elevada a cualquier tipo de exponente mayor que uno, se trata de una curva, que en algunos casos puede ser predecible, pero que otros se revela terriblemente caprichosa e imposible de dibujar si se carece de la técnica adecuada. Y aquí reside uno de los mayores méritos de Euler, el haber sido capaz de representar algunas funciones complicadas sin tener las herramientas analíticas adecuadas para ello.

Sumas infinitas

Euler introdujo un signo especial, que se ha seguido usando hasta la actualidad, para simbolizar una suma. Se trata de la letra sigma del alfabeto griego (Σ), que es la primera de la palabra suma.

Un sumatorio es una expresión del tipo

$$\sum_{i=1}^{i=5}$$

donde se especifica una variable, en este caso la i, y unos subíndices que nos indican la forma en que varía dicha variable. En el ejemplo, estos subíndices nos dicen que la i varía desde 1 hasta 5.

Es decir

$$\sum_{i=1}^{i=5} i = 1 + 2 + 3 + 4 + 5$$

$$\sum_{i=1}^{i=5} (n+1) = (1+1) + (2+1) + (3+1) + (4+1) + (5+1)$$

$$\sum_{i=1}^{i=5} n^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2$$

Es frecuente economizar poniendo en el índice superior sólo el final de la serie; de este modo,

$$\sum_{i=1}^{i=5} i = 1 + 2 + 3 + 4 + 5$$

indica que i varía desde 1 hasta 5.

Si el índice superior no es un número dado, sino el signo infinito, quiere decir que la suma tiene infinitos sumandos; por ejemplo:

$$\sum_{i=1}^{\infty} i = 1 + 2 + 3 + 4 + 5 + \cdots$$

Aunque en un principio pueda parecer extraño, hay sumas infinitas cuyo resultado final es un número finito (a este tipo de series se las llama «convergentes»). Por ejemplo, la serie

$$\sum_{i=1}^{\infty} \frac{i}{2^i} = \frac{1}{2} + \frac{2}{4} + \frac{3}{8} + \frac{4}{16} + \cdots$$

tiene una suma finita cuyo valor es 2. Intuitivamente podemos pensar que como los términos son cada vez más pequeños llegará un momento en que alguno estará tan próximo a cero que el resultado de la suma será un número finito. Es una manera de verlo, pero desde luego carece de cualquier precisión matemática. Por la misma regla de tres podríamos pensar que las series del tipo

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$

también tienen suma finita, pero no es así. Esta serie en concreto, en la que Euler estuvo especialmente interesado, recibe el nombre de «armónica»; gracias a ella obtuvo una demostración diferente de la que había dado Euclides para probar la existencia de infinitos números primos.

La serie armónica diverge, lo cual significa que la suma de sus términos vale infinito, pero lo hace de una forma extraordinariamente lenta, en comparación a como lo haría una serie del tipo

$$\sum_{n=1}^{\infty} n^2 = 1^2 + 2^2 + 3^2 + 4^2 + \cdots$$

Basándose en la serie armónica, Euler definió una función que habría de pasar a la historia como una de las más importantes que se han establecido en matemáticas, la «función zeta de Euler» (aunque actualmente recibe, algo injustamente, el nombre de «función zeta de Riemann»). Para definirla, Euler utilizó la letra griega ζ (zeta):

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \cdots + \frac{1}{n^x} + \cdots$$

Si hacemos que x = 1, se obtiene la serie armónica

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

que hemos visto con anterioridad, y la suma de cuyos términos sabemos que es igual a infinito. Sin embargo, Euler sospechaba que si hacía x = 2 la serie resultante,

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots$$

ya no tendería a infinito, dado que sólo había tomado de la serie armónica las fracciones en las que aparecían cuadrados. Calcular el valor de esta última serie era prácticamente imposible con los conocimientos de la época. Sin embargo, Euler, en uno de sus hallazgos más geniales, logró demostrar la siguiente igualdad:

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots = \frac{\pi^2}{6}$$

Euler realizó este descubrimiento a los 28 años, aunque no perfeccionó la demostración hasta seis años más tarde. La aparición repentina del número π, con el que se mide la longitud de la circunferencia, en el resultado de esta suma causó asombro en toda la comunidad matemática de la época. Con este hallazgo, Euler dio carpetazo a uno de los problemas abiertos más intrigantes del momento, el llamado «problema de Basilea».

El problema de Basilea

Jacob Bernoulli (1654-1705), junto con su hermano Johann (1667-1748), se dedicaron al estudio de las series armónicas, especialmente entre los años 1689 y 1704. Fueron ellos los que demostraron su divergencia. Animados por estos resultados estudiaron la serie formada por los inversos de los cuadrados:

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^2}$$

Jacob demostró que la serie convergía e incluso llegó a probar que la suma debía ser menor o igual que dos, pero no consiguió de ningún modo encontrar el valor exacto de dicha suma.



Johann Bernoulli fue maestro de Euler y uno de los mejores matemáticos de su época.

Su empeño fue tal que llegó a expresar que «grande será nuestra gratitud si alguien encuentra y nos comunica lo que hasta ahora ha escapado a nuestros esfuerzos». La cuestión fue conocida como «problema de Basilea», ya que ésta era la ciudad suiza en cuya universidad Johann tenía una cátedra de matemáticas y desde la cual se lanzó la famosa propuesta.

Ante este reto fracasaron matemáticos de la categoría de Mengoli y Leibniz, por no hablar de los denodados esfuerzos conjuntos que llevaron a cabo los hermanos Bernoulli. La solución, que llegó treinta años después, la obtuvo Euler, el «mago». El resultado fue realmente espectacular:

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots = \frac{\pi^2}{6}$$

Euler escribió al respecto: «... Sin embargo, he descubierto ahora y contra todo pronóstico una expresión elegante para la suma de la serie 1 + 1/4 + 1/9 + 1/16 + ..., que depende de la cuadratura del círculo... He encontrado que seis veces la suma de esta serie es igual al cuadrado de la longitud de la circunferencia cuyo diámetro es la unidad».

Por desgracia, Jacob ya había muerto cuando Euler publicó este resultado. « ¡Si viviera mi hermano!», *se lamentó Johann.*

El calificativo de «mago» atribuido a Euler responde al auténtico juego de magia matemática que supone la demostración. En realidad, no es nada complicada, pero requiere de ciertos conocimientos de matemáticas superiores, además de la audacia de Euler al tratar la serie en cuestión como si fuera una función polinómica, para luego relacionarla con el desarrollo en serie de la función seno; de ahí la aparición del número π, que es uno de los ceros de dicha función.

Jugando con la función zeta, Euler obtuvo diferentes resultados. Lo que sabía con seguridad era que cuando x tomaba valores menores o iguales a 1, el valor de la suma era infinito y que, por tanto, la serie sólo convergía para valores de x superiores a 1.

Euler pensó entonces en la posibilidad de hacer intervenir en la función a los números primos.

Sabía que el teorema fundamental de la aritmética de Euclides garantizaba que todo número natural se podía expresar de forma única como producto de números primos. Esto significaba que cada una de las fracciones que intervenía en la función zeta podía expresarse de manera tal que en el denominador sólo intervinieran números primos. Por ejemplo, supongamos que damos a la función zeta el valor x = 2:

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots + \frac{1}{n^2} + \cdots$$

y tomemos la fracción 1/360.

Hacemos la descomposición de 360 en factores primos 360 = 2^3 x 3^2 x 5, de manera que

$$\frac{1}{360} = \frac{1}{2^3}\frac{1}{3^2}\frac{1}{5^1}$$

Elevando al cuadrado los diferentes términos, obtenemos:

$$\left(\frac{1}{360}\right)^2 = \left(\frac{1}{2^3}\right)^2 \left(\frac{1}{3^2}\right)^2 \left(\frac{1}{5^1}\right)^2$$

Al hacer esta operación con cada uno de los denominadores de la función zeta, Euler llegó a la expresión

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \cdots + \frac{1}{n^x} + \cdots$$
$$= \left(1 + \frac{1}{2^x} + \frac{1}{4^x} + \frac{1}{8^x} + \cdots\right)\left(1 + \frac{1}{3^x} + \frac{1}{9^x} + \frac{1}{27^x} + \cdots\right)\left(1 + \frac{1}{p^x} + \frac{1}{(p^2)^x} + \frac{1}{(p^3)^x} + \cdots\right)$$

en la que ya sólo intervenían números primos. Se trata de una ecuación en la que en el término de la izquierda aparece una suma de infinitos números y en el de la derecha un producto, también de infinitos números, y que puede considerarse como la primera piedra en lo que iba a ser el edificio de la teoría analítica de números que se desarrollaría en los siglos posteriores. Esta expresión, que se conoce con el nombre de «producto de Euler», constituyó el punto de partida para que Riemann consiguiera, por primera vez, imponer un ritmo al caótico ejército de los números primos, tal como veremos en el capítulo 6.

Euler y el sonido

A Euler se le ocurrió introducir en la función llamada exponencial, definida por $f(x)= 2x$, una variable imaginaria. Su sorpresa fue mayúscula cuando se encontró con que en la gráfica de dicha función aparecían ondas, una serie de líneas sinuosas que eran las mismas que se encontraban cuando se intentaba representar sonidos musicales. En función de los valores que tomaran dichos números imaginarios, los sonidos se correspondían con notas más agudas o más graves.

Unos años más tarde, el matemático de origen francés Jean-Baptiste-Joseph Fourier (1768-1830) elaboró, basándose en el resultado obtenido por Euler, un sistema de análisis de las funciones periódicas que relacionan estrechamente los métodos analíticos con el mundo de los sonidos.

4. La conjetura de Goldbach

Christian Goldbach (1690-1764) fue un matemático prusiano que mantuvo una intensa correspondencia con Euler. El 18 de noviembre de 1752 le envió a éste una carta en la que afirmaba la siguiente proposición: «Todo número par mayor que 2 puede escribirse como suma de dos números primos». Cuando se dice aquí «suma de dos primos» se incluye el caso de que sea un número primo repetido dos veces. Por ejemplo:

$$4 = 2 + 2$$
$$6 = 3 + 3$$

$$8 = 3 + 5$$

$$10 = 3 + 7$$

$$12 = 5 + 7$$

$$14 = 3 + 11.$$

El 16 de diciembre del mismo año, Euler le contestó que había comprobado la conjetura hasta el número 1.000, y en otra carta fechada el 3 de abril de 1753, que había comprobado que el resultado era cierto hasta el número 2.500. Actualmente, la conjetura ha sido comprobada por métodos informáticos para todos los números pares menores de dos mil billones. La conjetura todavía no ha sido demostrada y está considerada por la comunidad matemática como uno de los problemas más difíciles de la historia de la ciencia.



Chen Jingrun (1933-1996), uno de los matemáticos más destacados del siglo XX, ofreció en 1966 el mejor resultado de la conjetura de Goldbach al demostrar que todo número par lo bastante grande puede escribirse como la suma de un primo y un semiprimo (número que es el producto, como mucho, de dos factores primos). Este hecho queda patente en el sello postal con el que la República Popular China distinguió a Chen en el año 1999, y en el cual, sobre la efigie del matemático, aparece su inecuación.

El tío Petros y la conjetura de Goldbach

Éste es el título de una famosa novela de Apostólos Doxiadis en la cual un matemático retirado propone a su sobrino que resuelva un problema de matemáticas. En el ánimo del protagonista está que su sobrino renuncie a estudiar la carrera de matemáticas si durante su periodo vacacional no consigue resolver el problema. Después de todo un verano de grandes esfuerzos, el sobrino desiste y se matricula en derecho. El problema propuesto era la conjetura de Goldbach. Con el fin de generar publicidad para el libro, el editor británico Tony Faber ofreció en el año 2000 un premio de un millón de dólares a aquel angloparlante que demostrase la conjetura antes de abril de 2002. Y, como era de esperar, nadie reclamó el premio.

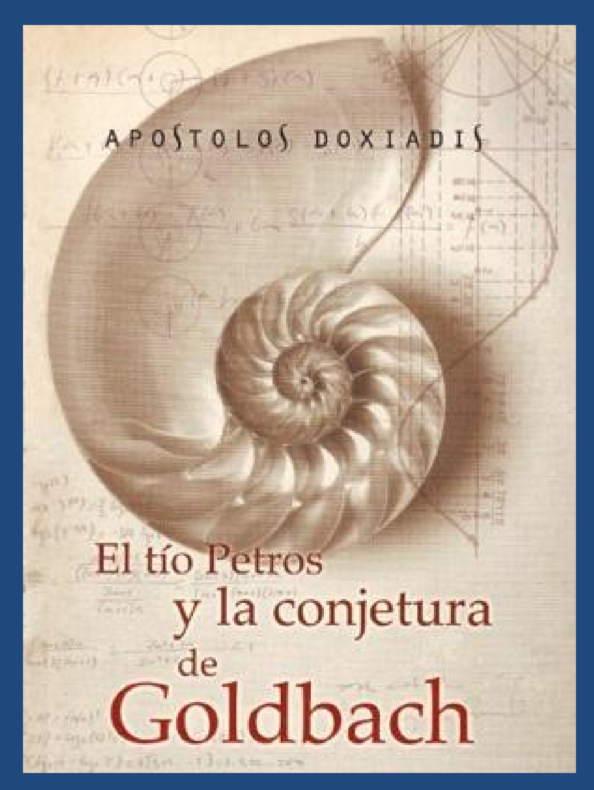


Ilustración de la portada de algunas ediciones del famoso libro de Apostólos Diodaxis, presidida por una concha de nautilus, plasmación en el mundo natural de una espiral logarítmica.

Capítulo 4
Logaritmos y números primos

Contenido:

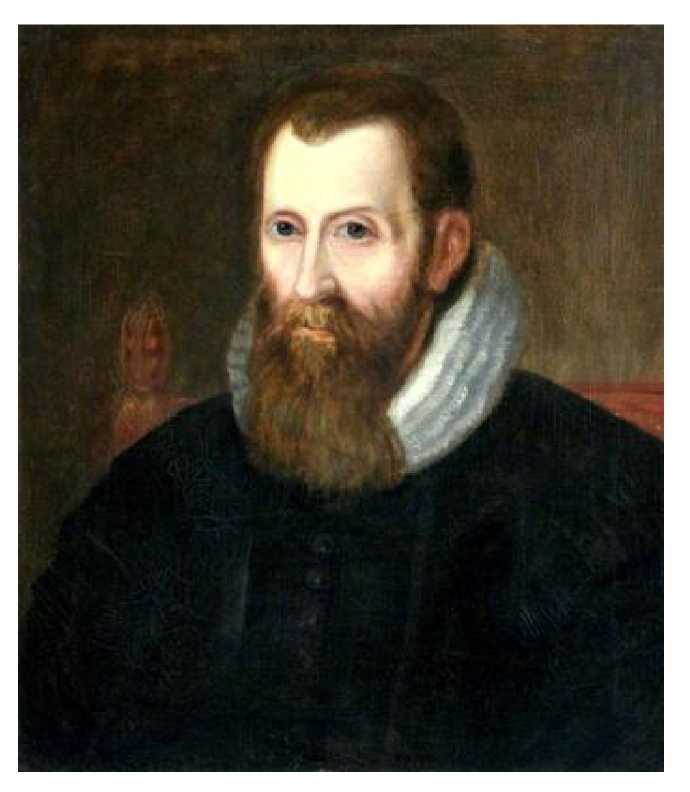
1. *John Napier*
2. *Johann Carl Friedrich Gauss*

En la investigación de un objeto, los dispositivos de los que nos servimos para su observación suelen tener un papel decisivo. El desarrollo de la astronomía ha estado vinculado al desarrollo tecnológico de los telescopios, así como la microbiología lo ha estado al de los microscopios. Los aparatos de observación, medición o detección han sido las llaves que han permitido abrir puertas a parajes desconocidos. En este sentido, las matemáticas no son una excepción: sus objetos de investigación se encuentran en el ámbito del pensamiento y, por tanto, no son dispositivos materiales, pero aún así tienen un alto nivel de concreción. Uno de los dispositivos matemáticos más poderosos que se han inventado han sido los logaritmos, que nacieron como un instrumento de cálculo, pero que, de la mano de Gauss, acabarían desempeñando un papel decisivo, como instrumento de observación, en la investigación de los números primos.

1. John Napier

En muchos textos pueden leerse referencias a logaritmos neperianos o logaritmos de Neper, mientras que en otros se habla de logaritmos de Napier. Y es que pocos nombres han tenido en la historia de las matemáticas tantas versiones diferentes: Napeir, Nepair, Nepeir, Neper, Napare, Naper, Naipper... Sin embargo, hay constancia de que el único nombre que el creador de los logaritmos no utilizó en toda su vida fue el de Napier, que en realidad era el verdadero.

John Napier nació en 1550 en el castillo de Merchiston, cerca de Edimburgo, Escocia. Era hijo de un noble, Archibald Napier, que gozaba de una excelente posición económica. John cursó estudios de teología en la Universidad de Saint-Andrews.

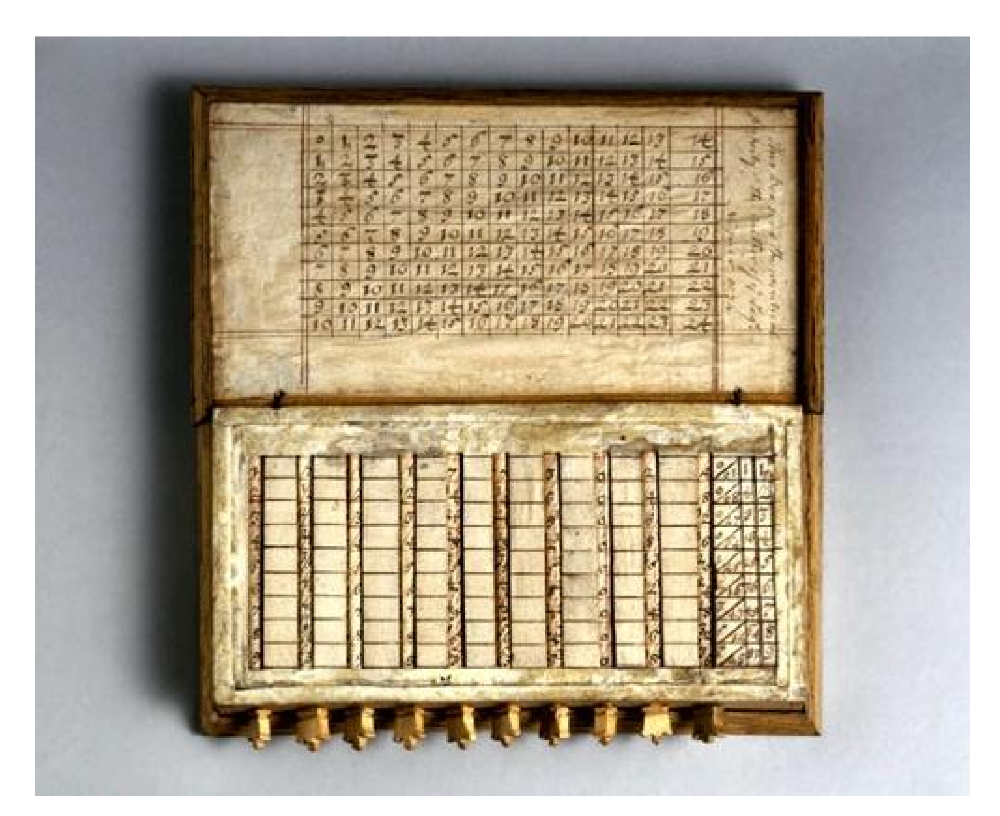


El matemático y teólogo escocés John Napier ha pasado a la historia por sus aportaciones a la simplificación del cálculo moderno.

Su interés por las matemáticas surgió a raíz de un largo viaje que llevó a cabo por Europa. Se tiene constancia de que estuvo en la Universidad de París y de que también pasó algún tiempo en Italia y Holanda. A su regreso a Escocia, en 1572, contrajo matrimonio con Elisabeth Stirling.

Durante los dos años siguientes se dedicó a la construcción de un castillo en Gartness. Napier pasó muchas horas encerrado en aquel castillo y fue en esa época cuando se entregó a sus misteriosos quehaceres matemáticos. Decimos misteriosos porque Napier, en las pocas ocasiones en que aparecía en público, lo hacía vestido de negro, llevando consigo un gallo, también negro, posado sobre su hombro. Toda esta escenografía le dio una fama de hechicero que quedó acrecentada por el hecho de hacer gala de una serie de conocimientos prácticos que nadie más poseía. Además de ser un destacado aficionado a las matemáticas, dedicó gran parte de su tiempo a investigar los evangelios, y especialmente el Apocalipsis de San Juan. Publicó las conclusiones a las que había llegado en una obra titulada *Plaine Discovery of the Whole Revelation of St. John* (*Los sencillos descubrimientos de la*

completa revelación de San Juan), que fue traducida a varios idiomas y en la que pretendía demostrar que el Papa de Roma era el anticristo.



Uno de los primeros modelos del ábaco neperiano, inventado por John Napier para el cálculo de productos y cocientes de números.

Extraños decimales

Que una fracción como 19/8 la expresemos como el número decimal 2,375 nos parece de lo más normal, basta con hacer la división de 19 entre 8. Pero en el siglo XVI las expresiones decimales eran realmente exóticas. Napier, que en su Descriptio *de 1614 ya se manifestaba a favor de las fracciones decimales, defendió enfáticamente en su obra* Constructio *(1619) el uso de la coma como signo de separación decimal en Inglaterra. Pero esta propuesta, así como la del ingeniero flamenco Stevin (1548-1620) de utilizar el sistema decimal para los pesos y medidas, no consiguió nunca imponerse ni en Inglaterra ni en Estados Unidos.*

Napier estaba interesado en la aritmología y en la astrología. Esta última lo llevó a investigar acerca de las propiedades de las figuras geométricas sobre una superficie esférica, obteniendo importantes resultados en la resolución de triángulos esféricos. Cualquier estudiante que haya abordado estudios de trigonometría esférica se habrá encontrado con más de una fórmula que lleva su nombre.

Sin embargo, para Napier había una cuestión que acabaría siendo prioritaria. En aquel tiempo, los cálculos numéricos eran sumamente engorrosos. Napier consideraba que podía dedicar su tiempo a hacer cosas más interesantes que llenar hojas y hojas con interminables cálculos que no suponían más que un trabajo puramente rutinario.

Llegó a inventar un dispositivo, confeccionado a base de varillas de sección cuadrada que se encastraban sobre unas tablas de multiplicar y que permitían realizar sumas y multiplicaciones con bastante facilidad. En 1617 publicó un manual titulado *Rabdologiae*, en el que explicaba cómo debía utilizarse. Esta herramienta, verdadera antecesora de la regla de cálculo, fue utilizada en Escocia durante más de cien años. Más adelante la perfeccionó sustituyendo las varillas por láminas perforadas, lo que permitía hacer multiplicaciones de números mucho mayores. De hecho, podría decirse que dichas láminas son un claro antecedente de las famosas tarjetas perforadas que aparecerían cuatro siglos más tarde con los primeros ordenadores IBM.

Sin embargo, la mayor creación de Napier, en lo que a la historia de las matemáticas se refiere, fueron los logaritmos, un ingenioso método de cálculo que publicó en 1614 bajo el título de *Mirifid logarithmorum canonis descriptio*.

Para evaluar el protagonismo que los logaritmos llegaron a tener en el estudio de los números primos es interesante recordar algunos de sus conceptos básicos.

Logaritmos

Los logaritmos parten de la siguiente idea: sabemos que 1.000 = 10 x 10 x 10, es decir, diez elevado a tres, que representamos en forma de potencia mediante 103, de manera que

$$1.000 = 10^3$$

$$10.000 = 10^4$$
$$1.000.000 = 10^6$$

Supongamos que queremos multiplicar estos tres números entre sí:

$$1.000 \times 10.000 \times 1.000.000 = 10.000.000.000.000.$$

Pero,

$$10.000.000.000.000 = 10^{13}.$$

Podríamos haber efectuado la multiplicación haciendo $10^{3+4+6} = 10^{13}$. Está claro que es más fácil sumar que multiplicar. Para convencernos, basta con hacer la multiplicación $10^{38} \times 10^{52} = 10^{90}$ a base de escribir ceros.

Pasemos ahora al lenguaje de los logaritmos. Con la igualdad $1.000 = 10^3$, nos podemos preguntar ¿a qué número debemos elevar 10 para que nos dé 1.000? La respuesta es 3. Esto lo escribiremos de la siguiente forma: log (1.000) = 3. De manera que, por ejemplo,

$$\log 100 = 2$$
$$\log 1.000 = 3$$
$$\log 1.000.000 = 6$$

La idea que subyace en este esquema es que es mucho más sencillo hacer sumas que productos.

Por ejemplo: log (100 x 1.000) = log 100 + log 1.000 = 2 + 3 = 5.

Por consiguiente, basta hacer el proceso inverso, el antilogaritmo, para obtener el resultado final: $10^5 = 100.000$.

Podríamos hacer todas estas operaciones mediante una tabla como la que se muestra a continuación:

1	10	100	1.000	10.000	100.000	1.000.000	10.000.000	100.000.000	1.000.000.000
0	1	2	3	4	5	6	7	8	9

La primera fila de esta tabla se ha construido empezando con el número 1, y cada nueva celda es igual a la anterior multiplicada por 10; es lo que se llama una progresión geométrica de razón 10.

En cambio, las celdas correspondientes a la segunda fila se obtienen de la anterior sumando una unidad. Lo más destacado es que así como en la fila de arriba se habla de productos, en la de abajo nos referimos a sumas. Según esto, la multiplicación

$$1.000 \times 100.000 = 100.000.000$$

es equivalente a la suma

$$3 + 5 = 8.$$

Podemos escribir una tabla como está poniendo en la primera fila la progresión geométrica que queramos, por ejemplo:

1	2	4	8	16	32	64	128	256
0	1	2	3	4	5	6	7	8

Para hacer el producto 4 x 16 debemos sumar en la fila de abajo 2 + 4. De forma análoga se pueden hacer divisiones, pero en este caso hay que tener en cuenta que el resultado equivale a la resta de los correspondientes números de la fila inferior. Por ejemplo, para calcular 256 dividido por 8, no tenemos más que hacer la resta 8 − 3 = 5, con lo que el resultado será 32, que es el número que hay la casilla superior del 5. En esta relación que existe entre los números de la fila inferior y los de la superior se encuentra, como decíamos antes, la clave del concepto de logaritmo.

Ahora ya podemos establecer una definición rigurosa de logaritmo. Cuando decimos que al 5 le corresponde el número 32, estamos expresando la igualdad:

$$2^5 = 32.$$

Recordemos que 2 elevado a 5 quiere decir 2 multiplicado por sí mismo cinco veces. Podríamos hacer una lectura de las dos filas de la última tabla de la forma siguiente: «3 es el número al que hay que elevar 2 para que de 8», y «7 es el número al que hay que elevar 2 para que de 128», lo que expresado abreviadamente se escribe así:

$$\log_2 8 = 3$$
$$\log_2 128 = 7$$

Estas expresiones se leen, respectivamente, «el logaritmo en base 2 de 8 es 3» y «el logaritmo en base 2 de 128 es 7». Si ahora tomamos como ejemplo la primera tabla tendríamos $10^4 = 10.000$, o sea, que 4 es el número al que hay que elevar 10 para que nos de 10.000. Expresado en forma de logaritmos, tendríamos $\log_{10} 10.000 = 4$, que se lee «el logaritmo en base 10 de 10.000 es 4».
Esto nos permite establecer una definición general de logaritmo: El logaritmo en base *a* de un número *b* es el número *c* al que hay que elevar la base a para que nos dé *b* ($a^c = b$), y lo escribiremos de la forma

$$\log_a b = c.$$

Napier estaba interesado en agilizar los cálculos en la trigonometría esférica y su idea de logaritmo estaba inicialmente aplicada a las funciones trigonométricas. Su planteamiento original no fue como el que hemos hecho nosotros, que se podría calificar de aritmético, sino de tipo cinemático, para lo que se planteó dos segmentos de recta que eran recorridos a diferentes velocidades. El término «logaritmo» fue empleado por primera vez por el mismo Napier y significa «número de la razón», en donde la palabra razón se refería a la relación que había entre los diferentes segmentos de las rectas utilizadas por Napier (en nuestro caso, a la relación que existe entre los números de la primera y la segunda fila de las tablas). Napier trabajó con logaritmos en base 10^7, que no era muy práctica. Además arrastraba, con bastante incomodidad, el hecho de que el logaritmo de 1 fuera cero,

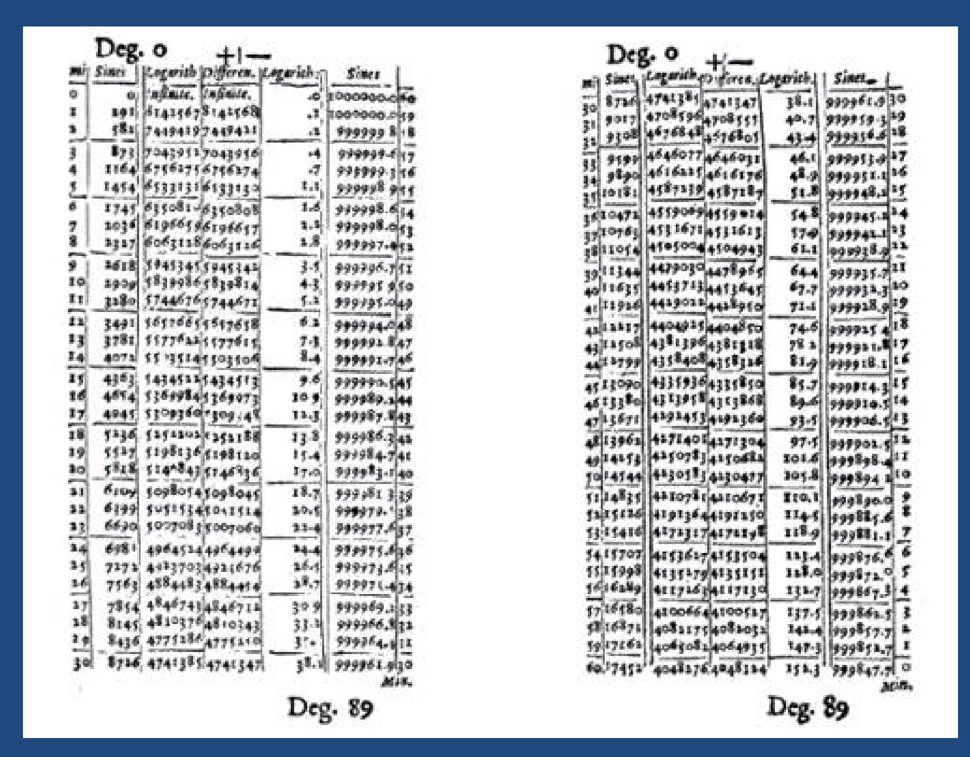
que era tanto como admitir que $10^0 = 1$. Henry Briggs (1561-1630), titular de la cátedra de geometría de Oxford, le escribió una carta comunicándole el interés que había despertado en él el tema de los logaritmos y sugiriéndole un encuentro. En el verano de 1616 Briggs se reunió con Napier en su castillo de Merchiston y discutieron la posibilidad de utilizar el número 10 como base y de que log 1 = 0. Napier, que por aquel entonces ya estaba enfermo, rehusó emprender una nueva versión de sus tablas de logaritmos. Napier murió al año siguiente y Briggs planteó entonces una definición de logaritmo muy similar a la expresada aquí, dando lugar al nacimiento, de lo que se conocen como «logaritmos de Briggs».

Pero un hecho aparentemente casual en la confección de tablas de logaritmos iba a marcar un hito en la historia de las matemáticas. De la misma forma que en las libretas escolares existía la costumbre de poner en la contraportada las tablas de multiplicar, en la mayoría de las tablas de logaritmos se adjuntaba al final una Esta de números primos. El asunto puede tener una explicación bastante plausible: si tenemos en cuenta que cualquier número se puede expresar como un producto de factores primos, lo lógico es calcular primero el logaritmo de los números primos y a continuación obtener los logaritmos de los demás números mediante simples sumas. El caso es que en las tablas de logaritmos que Gauss utilizó en el colegio había al final una lista de los mil primeros números primos. Una mente prodigiosa estaba frente a dos conceptos aparentemente inconexos y de su alquimia posterior nacería uno de los teoremas más interesantes del álgebra.

Tablas logarítmicas

Actualmente, el cálculo de un logaritmo se reduce a pulsar una tecla en una sencilla calculadora de bolsillo, pero en el siglo XVII se necesitaba estar en posesión de grandes volúmenes que contuvieran los logaritmos de la mayor cantidad de números posible. En 1617 Briggs publicó las primeras tablas en las que podían encontrarse los logaritmos de los números comprendidos entre 1 y 1.000 con una precisión de catorce decimales. Siete años después aparecerían unas nuevas tablas, primero con valores comprendidos entre 1 y 20.000 y entre 90.000 y 100.000, también con una aproximación de catorce decimales. En muy poco tiempo se llevaron a cabo ediciones de

estas tablas en varios países, dado el enorme valor práctico que suponía el cálculo mediante logaritmos: la navegación marítima requería disponer de cartas astronómicas cada vez más precisas, pues la complejidad de cálculos trigonométricos que esto suponía a los astrónomos los llevaba a emplear horas, días e incluso años. Como diría Laplace: «Gracias a sus trabajos (de Napier) se alargó al doble la vida de los astrónomos»



Las primeras tablas de logaritmos, asociadas a los cálculos de trigonometría esférica de Napier, se publicaron en Edimburgo en 1614.

2. Johann Carl Friedrich Gauss

Gauss nació en Brunswick, Alemania, el 30 de abril de 1777. Era de origen humilde y su futuro, si nada ni nadie lo remediaba, estaba destinado a las labores del campo. Pero ya en la escuela primaria Gauss dio la nota con tan sólo nueve años.



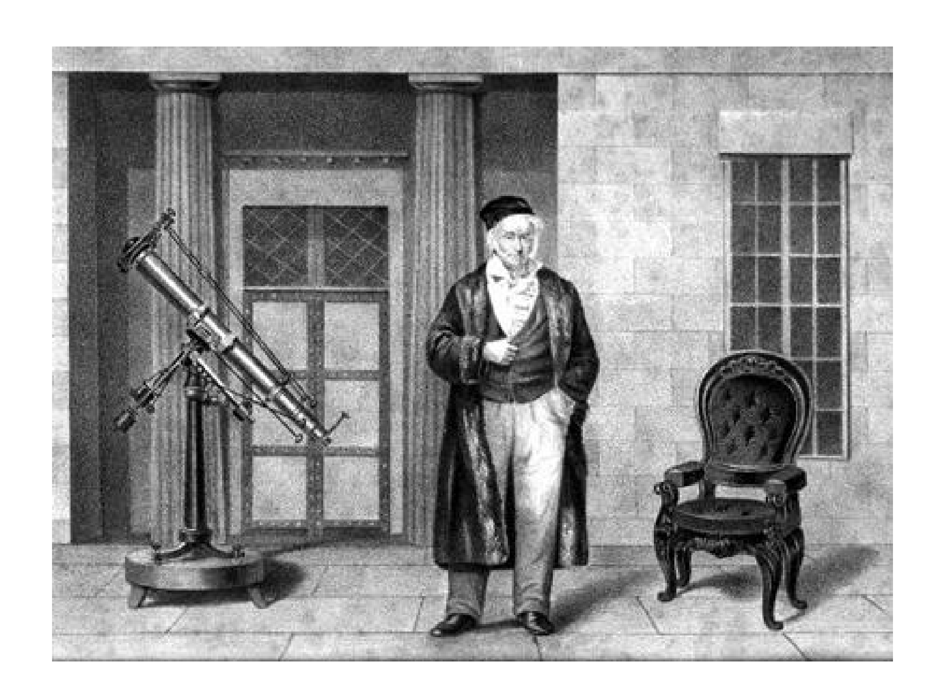
Retrato de juventud de Gauss.

Se trataba de una escuela rural con escasos medios en la que el maestro, que se llamaba Büttner, se veía obligado a mantener ocupados a cerca de un centenar de alumnos. Una manera fácil de hacerlo era obligarlos a realizar pesados cálculos rutinarios. En una ocasión les hizo calcular la suma de los cien primeros números. Al cabo de un instante Gauss dejó su cuaderno encima de su mesa y exclamó: « ¡Ya está!». Gauss no sólo había hecho la suma

$$1 + 2 + 3 + 4 + \ldots + 100 =$$
$$= (1 + 100) + (2 + 99) + (3 + 98) + \ldots + (50 + 51) =$$
$$= 101 + 101 + \ldots + 101 =$$
$$= 101 \times 50 = 5.050$$

en una velocidad récord, sino que también había resuelto el problema de la suma de los términos de una progresión aritmética. Büttner se dio cuenta enseguida de que estaba ante un alumno especialmente dotado y decidió presentarle a Johann Martin Bartels (1769-1836), un alumno apasionado por las matemáticas ocho años mayor

que Gauss, con el que empezaría a dar sus primeros pasos por el mundo de los números y con el que mantuvo una profunda amistad durante toda su vida. La madre de Gauss, Dorothea Benz, consciente de que debía hacer algo para que las extraordinarias aptitudes de su hijo recibieran la ayuda que sus padres no podían darle, se puso en contacto con el que habría de ser su protector, el duque de Brunswick, que le consiguió las becas necesarias para sus estudios en el liceo y, posteriormente, en la Universidad de Gotinga. De este modo, el joven Gauss consiguió salir del ámbito rural para convertirse en el «príncipe de las matemáticas». Su carrera profesional culminó cuando le otorgaron el título de catedrático de astronomía y director del observatorio astronómico de la Universidad de Gotinga. La vida de Gauss transcurrió de una forma razonablemente apacible. Mantuvo, por respeto al duque, su protector, un talante conservador en una época de cierta agitación política. Era hijo único y no se casó hasta los 32 años. Lo hizo con Johanna Osthoff, con quien tuvo tres hijos, el tercero de los cuales falleció a los pocos meses de morir la madre. Gauss volvió a contraer matrimonio en 1810 con Wilhelmine Waldeck, hija de un catedrático de derecho, matrimonio del que nacieron tres hijos más. El 23 de febrero de 1855 Gauss murió en la ciudad de Gotinga. Por entonces, su fama Monumento a Gauss y Weber en Gotinga como científico ya había dado la vuelta al mundo.



Litografía obra de Eduard Ritmüller en la que aparece Gauss en la terraza del observatorio de la Universidad de Gotinga.

Un científico completo

Gauss también llevó a cabo diversos trabajos fuera del ámbito de las matemáticas. Son destacables los resultados que obtuvo sobre el magnetismo terrestre, el electromagnetismo, la capilaridad, la atracción de los elipsoides y la dióptrica. En sus trabajos sobre geodesia, se debe a Gauss, entre otras cosas, el invento del heliotropo (un aparato para transmitir señales mediante la luz reflejada). Una anécdota curiosa respecto a estas investigaciones ocurrió en 1833, cuando Gauss trabajaba conjuntamente con Wilhelm Weber (1804-1891) en investigaciones electromagnéticas. Para poder enviarse mensajes con rapidez, Gauss construyó, con sus propias manos, un aparato eléctrico capaz de transportar mensajes a la velocidad de la luz. Habla inventado, nada más y nada menos, que el telégrafo eléctrico.



Monumento a Gauss y Weber en Gotinga

La primera conjetura

En la libreta de apuntes que Gauss utilizaba a los 14 años puede leerse la nota

«Números primos menores que *a* (= ∞) *a*/l*a*».

Gauss se había concentrado en el estudio de la larga lista de números primos que figuraba al final de su tabla de logaritmos, y era inevitable que acabara atrapado en el hechizo de la caótica serie. Pero ya había decidido que sus pasos no iban a estar encaminados a encontrar una fórmula que le permitiera saber cómo era y dónde estaba «el siguiente número primo». Presentía claramente que ése era un camino que lo abocaría al fracaso. En vez de esto, lo que hizo fue calcular cuántos números primos había entre dos números dados o, más exactamente, cuantos números primos había entre los diez, los cien, los mil, los diez mil primeros números, ya que de esta forma podría estimar la frecuencia de aparición de los números primos entre la serie de los números naturales. Sabemos que entre los diez primeros números naturales tenemos sólo cuatro números primos (2, 3, 5 y 7). Entre diez y cien aparecen veintiuno. Para expresar esto, Gauss definió una función a la que llamó *k(x)* y que definió de la siguiente forma:

π (x) = la cantidad de números primos que son menores que x.

Según esto, π (10) = 4.

Por ejemplo, para calcular π(15), tendríamos que contar los números primos que hay menores que 15, que son 2, 3, 5, 7, 11, 13, con lo que π (15) = 6.

El símbolo π que aparece en la fórmula es el conocido número pi, pero en este contexto carece de significado matemático, ya que la función podría definirse de la misma forma si pusiéramos cualquier otro símbolo, como C(x). La verdad es que la elección de π no fue muy afortunada por parte de Gauss, y es probable que cogiera lo primero que le vino a la cabeza. Decimos que no fue muy afortunada porque la visión de π(x) sugiere de forma automática todo tipo de relaciones matemáticas con la circunferencia que son completamente ajenas, en este contexto, al tema de los

números primos. En cualquier caso, aquí seguiremos utilizando la notación de Gauss.

El matemático alemán construyó entonces una primera tabla de dos columnas, de manera que en la primera puso las potencias de 10 y en la segunda, el valor que tomaba π(x).

La siguiente tabla está calculada para los diez mil primeros millones. Obviamente, en la época de Gauss las herramientas de cálculo eran mucho más precarias y no disponía de semejante rango de valores.

x	π (x)
10	4
100	25
1.000	168
10.000	1229
100.000	9.592
1.000.000	78.498
10.000.000	664.579
100.000.000	5.761.455
1.000.000.000	50.847.534
10.000.000.000	455.052.512

Lógicamente, π(x) es un número que va aumentando, pero la forma de hacerlo no nos dice gran cosa. Vamos a añadir otra columna que nos dé la proporción de números primos menores que otro dado. Para ello calculamos el cociente

$$\frac{\pi(x)}{x}$$

Sabemos que hay 168 números primos menores que 1.000:

$$\frac{\pi(x)}{x} = \frac{\pi(1000)}{1000} = \frac{168}{1000} = 0{,}168$$

El dato que nos proporciona este número es que el 16,8% de los números que hay entre 1 y 1.000 son primos. El 83,2% restante está formado por números compuestos. Al añadir esta tercera columna a la tabla

x	π(*x*)	π (*x*)/*x*
10	4	0,40000000
100	25	0,25000000
1.000	168	0,16800000
10.000	1.229	0,12290000
100.000	9.592	0,09592000
1.000.000	78.498	0,07849800
10.000.000	664.579	0,06645790
100.000.000	5.761.455	0,05761455
1.000.000.000	50.847.534	0,05084753
10.000.000.000	455.052.512	0,04550525

podemos observar que la proporción de números primos va disminuyendo conforme vamos avanzando hacia números más grandes. Esto ya empieza a ser un lato, lo que ocurre es que era un dato predecible. Para que un número sea primo no puede ser divisible por ninguno de los que le preceden. Para que, por ejemplo, 3 sea primo, no debe ser divisible por 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 y 12. Cuanto mayor sea el número, más alta es la exigencia de no ser divisible y, por lo tanto, es lógico que los números primos vayan escaseando cada vez más. Pero Gauss ya sabía que eso no significaba que pudiera llegar un momento en que se acabaran los números primos disponibles, pues conocía perfectamente la existencia del teorema fundamental de la aritmética con el que Euclides había demostrado la infinitud de los números primos.

La tercera columna que incluyó Gauss en la tabla no fue la que se obtenía haciendo el cociente

$$\frac{x}{\pi(x)}$$[1]

sino el inverso

$$\frac{x}{\pi(x)}$$

x	π(x)	*x*/π(x)
10	4	2,5
100	25	4
1.000	168	6
10.000	1.229	8,1
100.000	9.592	10,4
1.000.000	78.498	12,7
10.000.000	664.579	15
100.000.000	5.761.455	17,4
1.000.000.000	50.847.534	19,7
10.000.000.000	455.052.512	22

Esta tabla nos indica, por ejemplo, que entre los cien primeros números, uno de cada cuatro es primo; que entre los mil primeros números alrededor de uno de cada seis es primo, y así sucesivamente. Esto es simplemente una estimación. La tabla no afirma que entre los cien primeros números aparezca un número primo cada cuatro números, algo que podemos comprobar de forma rápida consultando la criba de Eratóstenes para los primeros cien números. De manera que la tabla anterior más bien debe interpretarse como una distancia probable entre números primos.

Gauss observó que la última columna crecía aproximadamente en dos unidades cada vez que avanzaba una fila. De manera que la situación era la siguiente: si multiplicaba por diez en la primera fila, debía sumar dos en la segunda. Esta relación entre producto y suma se encontraba implícita en la propia naturaleza de

[1] Así lo indica el original, pero al parecer es el inverso. Nota PB

los logaritmos. Gauss tenía en las manos una tabla de logaritmos y otra de números primos en un mismo volumen. Ello le dio la idea para hacerse con una herramienta diferente, un nuevo dispositivo de observación. Los logaritmos se iban a convertir en la nueva lente que Gauss adaptaría a su telescopio. Como ya hemos visto, cuando la base de los logaritmos es 10, cada vez que se multiplica por 10, los logaritmos decimales aumentan de uno en uno, por lo que esta base no iba bien al esquema de Gauss y decidió tomar logaritmos en base e, un número de características similares a las del número π. Su valor aproximado es

$$e = 2{,}7182818284590452354...$$

Se trata de una expresión decimal infinita y aparece en matemáticas con tanta o más frecuencia que el número π, por lo que cuando se toma un logaritmo en base *e* se dice que se está tratando con «logaritmos naturales». Tal como ya se ha explicado, deberíamos escribir $\log_e$ para simbolizar los logaritmos naturales; sin embargo, se escriben de forma abreviada como «ln». En las calculadoras científicas hay una tecla para «log», logaritmo decimal, y otra para «ln», logaritmo en base *e*.
La conjetura que hizo Gauss a partir de este punto fue la siguiente:
Para valores grandes de x, el valor de π(x)/x se aproxima a 1/ln x, lo que expresado de otra forma sería

$$\frac{\pi(x)}{x} \approx \frac{1}{\ln x}$$

(para valores grandes de x)

Este resultado da una estimación de la frecuencia con que aparecen los números primos en la sucesión de los números naturales. Supongamos que *P*(*N*) es el número de primos menores que *N*; la fórmula afirma que conforme aumenta N, el cociente *N*/*P*(*N*) se acerca cada vez más al logaritmo natural de *N*.
Existe una manera sencilla de poner en práctica la fórmula de Gauss cuando queremos conocer cuántos números primos hay menores que uno dado. Por

ejemplo, supongamos que alguien nos hace la siguiente pregunta: ¿cuántos números primos crees que hay entre los mil primeros números? Tomamos una calculadora de bolsillo y hacemos los siguientes pasos:

1. Introducimos el número 1.000;
2. pulsamos la tecla ln;
3. luego la tecla 1/x;
4. multiplicamos el resultado por 1.000
5. ... y aparece el número 144,76482730108394255037630630554

que nos permite responder afirmativamente a la pregunta: «¿Habrá unos 145 números primos entre el 1 y el 1.000?». La aproximación no es ninguna maravilla porque, en realidad, hay 168.

Pero no olvidemos que el teorema se va afinando conforme el número N se va haciendo más grande, y nos puede permitir afirmar con cierta tranquilidad, por ejemplo, que sólo el 3,6% del primer billón de números son primos.

Ahora ya podemos descifrar lo que quería decir Gauss cuando escribió «Números primos menores que a (= ∞) a/la» en su libreta de apuntes:

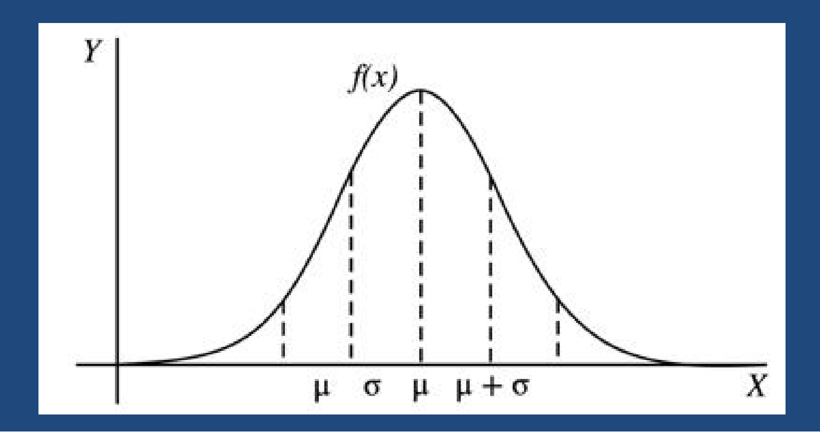
- «números primos menores que a» significa lo mismo que π(a).
- «la» es lo que hemos puesto como ln a.
- « = ∞» significa que la igualdad es válida para valores muy grandes de *a* (cuando *a* tiende a infinito).

La campana de Gauss

A los 18 años, Gauss habla descubierto el método de los mínimos cuadrados, despertando en él un interés especial por la teoría de errores. Creó entonces un método de observación estadística, en el que la distribución normal de los errores seguía una curva en forma de campana. Sin duda, la más popular de las curvas que hay en matemáticas y que recibe el nombre de «campana de Gauss».

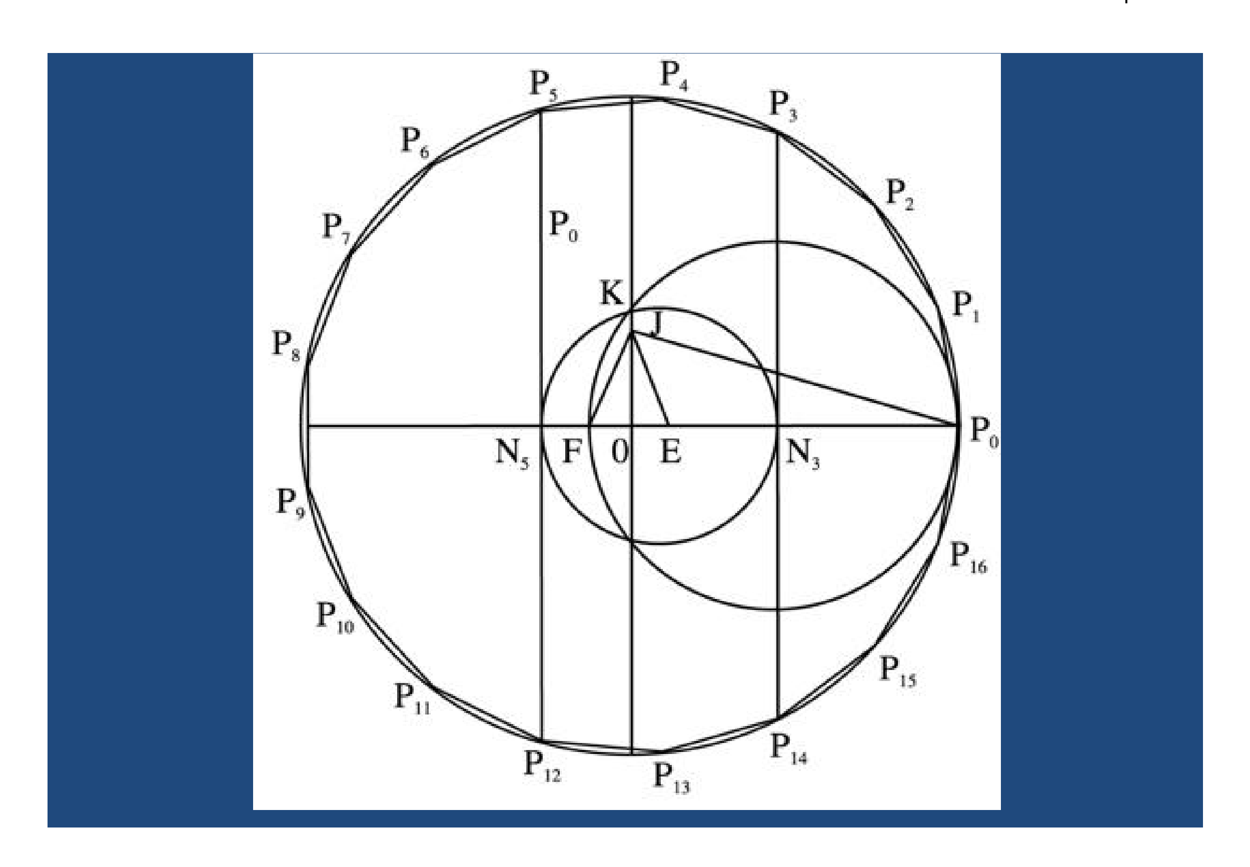
Este método de observación acabó por producirle un rendimiento muy beneficioso, ya que Gauss inició un estudio sistemático de los movimientos bursátiles internacionales que figuraban en la prensa extranjera que

llegaba regularmente a la sala de lecturas de la universidad. La campana de Gauss sonó y los beneficios que obtuvo fruto de esta investigación superaron con creces su sueldo de catedrático.



El polígono de Gauss

La construcción de polígonos regulares con regla y compás había sido un problema sin resolver desde el tiempo de los geómetras griegos. Se sabía cómo construir los de tres, cuatro, cinco y quince lados, así como las duplicaciones de éstos. El 30 de marzo de 1796, Gauss descubrió la forma en la que debía construirse el polígono de diecisiete lados. Fue una fecha trascendente en su biografía, ya que ese mismo día empezó su diario científico, que abarca el periodo 1796-1814, y que está considerado como una auténtica joya de las matemáticas, ya que en él se encuentran anotados todos sus hallazgos científicos. Pero quizás aún más importante sea el hecho de que, en esa misma fecha, Gauss decidió dedicarse a las matemáticas en vez de a la filología, rama esta última en la que había dado pruebas de genialidad.



Hoy día este resultado se conoce como «teorema de los números primos», y es uno de los más importantes de la historia de las matemáticas. La alocada banda de los números primos empezaba a encontrar la horma de su zapato. En su estudio se había introducido una «función», que era tanto como encaminarlo por una autopista que, con el tiempo, tendría cada vez mejor definidas sus normas de circulación.

Gauss no dio a conocer este resultado. Los motivos no se debieron a una actitud de mezquina reserva, como se ha dado con más frecuencia de la deseada en muchos ámbitos del conocimiento, ni tampoco en la vertiente de Fermat, que hubiera aducido que no incluía la demostración por ser demasiado larga. En este último sentido podríamos afirmar que Gauss disponía de suficiente papel para incluir cualquier demostración por larga que fuera. Gauss no dio a conocer este teorema precisamente porque no tenía ninguna manera de demostrarlo. Las matemáticas habían dado un giro que ya se apuntaba con Euler. La teoría matemática debía estar incuestionablemente articulada en un escenario lógico que empezaba a abrirse camino entre técnicas ambiguas y pragmatismos dudosos. La intuición, eje troncal de cualquier descubrimiento, debía apoyarse en sólidas bases teóricas. La

demostración de un teorema se había convertido en una argumentación objetiva que, gracias a un lenguaje común, adquiría la categoría de verdad.

La conjetura de Gauss no se convertiría en teorema hasta cien años más tarde: en 1896, Jacques Hadamard (1865-1963) y C. J. de la Vallée Poussin (1866-1962) demostraron el teorema simultáneamente, pero de forma independiente, por lo que el mérito debe atribuirse a ambos. De entre los muchos teoremas que se han creado en torno a los números primos, el que Gauss inició con su conjetura ocupa un lugar de honor en la historia de las matemáticas, no sólo por su belleza, sino también por la enorme importancia que ha tenido en el desarrollo posterior de la investigación de los números primos.



En el anverso de este billete de diez marcos, Gauss aparece junto a la curva conocida como «campana de Gauss». En el reverso se reproduce un sextante,

instrumento empleado para establecer una de las primeras redes geodésicas del mundo, en la región de Hamburgo, tal como se representa en la esquina inferior derecha. La noción de «geodésica», o línea de menor longitud que une dos puntos de una superficie dada, es un concepto clave en geometría y fue otra más de las aportaciones científicas del asombroso genio alemán.

Capítulo 5
Las piedras angulares

Contenido:

1. *Sumas mágicas*
2. *El reloj de Gauss*
3. *Números imaginarios*
4. *Una dimensión más*

Tres son los desarrollos teóricos que constituyen los pilares fundamentales sobre los que se construye el estudio moderno de los números primos: la aritmética modular, los números complejos y la teoría analítica de funciones. La tercera es la que precisa mayores conocimientos matemáticos para poder ser abordada. Sin embargo, hay un aspecto de la misma, el esfuerzo para poder «ver» una función cuya representación requiere un espacio de cuatro dimensiones, que se puede comprender fácilmente y que ayuda a entender el modo en que la función zeta de Riemann consiguió, por fin, imponer un ritmo a la caótica sucesión de los números primos.

1. Sumas mágicas

Como es sabido, los números tienen una simbología, más o menos precisa, que adopta diferentes versiones según la corriente mística que los apadrina. La mayoría de estos símbolos, por lo menos en el mundo occidental, tiene un tronco común en la Biblia y también en las escuelas pitagóricas.

«Todo lo cognoscible tiene un número, pues no es posible que sin número algo pueda ser concebido o conocido», afirmaba Filolao (Crotona, n. 480 a. C.), matemático y filósofo griego que fue discípulo de Pitágoras.

Números y letras

En las culturas griega y hebrea también las letras tenían asociados números, de manera que las palabras podían adquirir diferentes significados místicos. La operación básica consistía en sumar los números

que estaban asociados a cada letra. Para comparar dos palabras se comparaban los números correspondientes, y la que daba una cantidad mayor se consideraba más importante. Cuenta la leyenda que la superioridad de Aquiles frente a Héctor procedía de este cálculo: la palabra Aquiles sumaba 1.276, mientras que Héctor daba como resultado sólo 1.125.

La transmisión de esta «cultura numérica» se vio muy entorpecida cuando se introdujo en los oscuros pasillos de la Edad Media. La Iglesia católica hizo una clara distinción entre las diferentes concepciones filosóficas del mundo y los principios inamovibles que conformaban su doctrina.

Uno de los vehículos que consiguió, hasta cierto punto, traspasar los muros de la intolerancia fue el juego del tarot. Aunque también la Iglesia acabó condenándolo, su aritmología se preservó en muchos textos de carácter ambiguo en los que no se sabía muy bien si se hablaba de ritos adivinatorios o de aritmética.

Basado en un sistema de numeración decimal, el tarot asigna a cada uno de los nueve primeros números significados especiales. Parte del número 1, de la unidad como principio único, y del 2 como símbolo de la polaridad y, por tanto, de la generación. El 3 es la dirección que toma el 2 mediante la suma 2 + 1. El siete, por tomar otro ejemplo, representa la acción del uno, que desarrolla la potencia contenida en el seis: 7 = 6 + 1. Y así sucesivamente.

De esta forma, partiendo de la unidad, se adjudican principios básicos a los nueve primeros números, y cualquier otro debe poder ser reducido a alguno de éstos. Es entonces cuando se define la llamada «suma mágica». La idea básica consiste en sumar todas las cifras que componen el número en cuestión para reducirlo a una única cifra. Tomemos como ejemplo el número 47; éste se reduce haciendo 4 + 7 = 11 = 1 + 1 = 2. De esta forma, el número 47 es heredero de la simbología del número 2 pero situado en un plano superior. Otras reducciones serían, por ejemplo

$$157 = 1 + 5 + 7 = 13 = 1 + 3 = 4$$

Las operaciones básicas de suma y producto se harían también por reducción. Por consiguiente, para sumar los números 248 y 396 podemos hacer primero las reducciones

$$248 = 2 + 4 + 8 = 14 = 1 + 4 = 5$$

y

$$396 = 3 + 9 + 6 = 18 = 1 + 8 = 9,$$

de manera que las suma de estos dos números sería

$$9 + 5 = 14 = 1 + 4 = 5$$

Si, en vez de esto, primero efectuamos la operación suma y luego reducimos el resultado obtenemos

$$248 + 396 = 644 = 6 + 4 + 4 = 14 = 1 + 4 = 5$$

Se comprueba así que esta operación de reducción mantiene los resultados de la suma. Análogamente, para un producto de dos números observamos que sucede lo mismo:

$$45 \times 27 = 1.215 = 1 + 2 + 1 + 5 = 9$$

$$45 = 4 + 5 = 9$$

$$27 = 2 + 7 = 9$$

$$9 \times 9 = 81 = 8 + 1 = 9$$

Si, según este criterio, disponemos ahora todos los números naturales en columnas, de manera que en cada columna figuren todos aquellos que, según la suma mágica, son equivalentes, tendríamos:

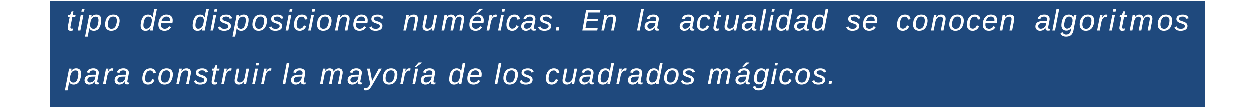
1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54
55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81
82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99
100	...	...	...	...	...	...	...	...

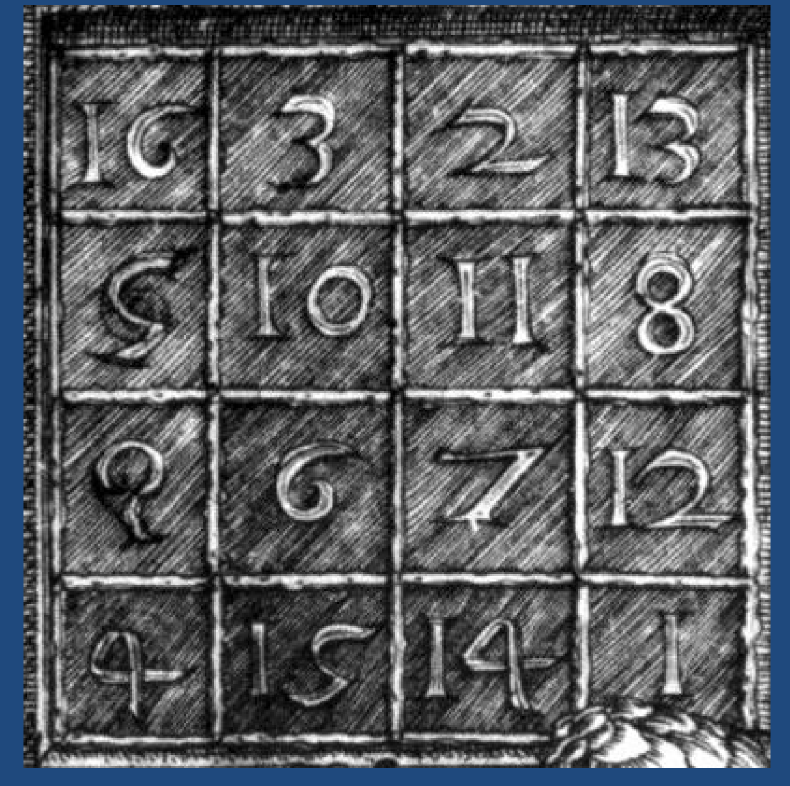
Ahora podemos decir que 78 se encuentra en el grupo del 6, o bien que 93 está en el del 3. En el lenguaje matemático actual, a estos grupos se los denomina «clases de equivalencia». Se habla, por consiguiente, de la «clase del 3», la «clase del 5», etcétera.

Este tipo de clasificaciones, que ya era conocido por los matemáticos, llevó a Gauss a construir una nueva herramienta de cálculo que acabó revelándose muy útil a la hora de determinar algunas de las características de los números primos

El cuadrado mágico

Por «suma mágica» también se suele entender la operación suma que se lleva a cabo en los cuadrados mágicos (una disposición de números en forma de cuadrado de manera tal que la suma de filas, columnas o diagonales dé siempre el mismo resultado). La mayoría de las culturas han desarrollado cuadrados mágicos. Muchos matemáticos de renombre, como Stifel, Fermat, Pascal, Leibniz o el mismo Euler, se han interesado por este


tipo de disposiciones numéricas. En la actualidad se conocen algoritmos para construir la mayoría de los cuadrados mágicos.



Cuadrado mágico representado en el cuadro Melancolía I, obra del pintor renacentista Alberto Durero.

2. El reloj de Gauss

La esfera de un reloj tiene doce números distribuidos en el perímetro de un círculo. Después del número 12 debería venir el 13, pero lo que hacemos es volver a contar desde el principio. El esquema es prácticamente el mismo que el que hemos explicado al introducir el método de las sumas mágicas, con la diferencia de que ahora, en vez de empezar a contar a partir del 9, lo hacemos a partir del 12. Podríamos construir una tabla similar a la anterior, pero que en vez de nueve columnas tuviera doce. Vamos a escribir únicamente las dos primeras filas de esta tabla:

1	2	3	4	5	6	7	8	9	10	11	12

13	14	15	16	17	18	19	20	21	22	23	24
...	...	...	...	...	...	...	...	...	...	...	...

Esta operación la llevamos a cabo cada día cuando miramos el reloj, ya que para distinguir las horas que preceden al mediodía de las que le siguen es habitual seguir contando a partir del número 12. Por ejemplo, cuando nos referimos a las 17 horas entendemos que equivale a las «5 de la tarde», por lo que en este sentido sabemos que el número 17 es de la misma «clase» que el 5. A partir de aquí, lo que Gauss se plantea son diferentes relojes, o, más exactamente, diferentes cuadrantes. Por ejemplo, un reloj que tenga sólo cinco horas nos daría una tabla del tipo:

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
...	...	...	...	...

De manera que, según el criterio que hemos establecido antes, podemos decir que el número 17 es del grupo del 2 ó, hablando con más propiedad, que pertenece a la «clase» del 2.

Es fácil saber a qué clase pertenece un número cualquiera. Por ejemplo, el 18: tendríamos que dar 3 vueltas a nuestro reloj de 5 horas para sumar 15 y luego empezar de nuevo hasta llegar al número 3, de modo que pertenece a la clase del 3. Esto es lo mismo que dividir 18 entre 5 y quedarnos con el resto de la división que es 3. Esta operación es muy práctica cuando se trata de números grandes. Si queremos saber a qué clase pertenece el número 40.248, lo dividimos entre 5, lo que nos da un cociente de 8.049 y un resto de 3; por tanto, pertenece a la clase del 3. Como los múltiplos de 5 dan todos de resto 0, al dividirlos entre 5, lo que se hace es llamar 0 a la clase del 5, con lo que la tabla anterior quedaría de la forma:

0	1	2	3	4
10	6	7	8	9

15	11	12	13	14
20	16	17	18	19
...	...	...	...	...

Podríamos decir que 17 es lo mismo que 2, pero una igualdad como 17 = 2 se podría prestar a confusión, por lo que se suele poner de la forma 17 ≡ 2.

Podemos convenir en que una expresión así es correcta, pero es obvio que hay que añadir un dato: es necesario saber en qué tipo de reloj nos estamos moviendo. En este caso concreto es un reloj en el que sólo hay cinco números en el cuadrante, lo que indicamos poniendo a la derecha *mod* 5, con lo que la expresión anterior quedaría definitivamente de la siguiente manera:

$$17 \equiv 2 \ (mod\ 5).$$

Esta expresión es lo mismo que decir que 17 y 2 son equivalentes en módulo 5. Como era habitual en la época, Gauss utilizaba el latín para sus escritos científicos, motivo por el cual adoptó el vocablo módulo (ablativo de *modulus*). En ese momento tuvo lugar el nacimiento de lo que actualmente conocemos como aritmética modular, una de las herramientas más poderosas de la teoría de números.

Congruencias

En aritmética modular se habla de congruencias en vez de igualdades, de manera que la forma correcta de referirse a la expresión anterior es «17 es congruente con 2 módulo 5». Para saber si dos números cualesquiera son congruentes módulo 5 basta con hacer la diferencia y ver si el resultado es múltiplo de 5. En el ejemplo anterior tendríamos 17 – 2 = 15, que es múltiplo de 5.

82 = 58 (*mod* 4) porque 82 – 58 = 24, que es múltiplo de 4.

Una vez establecido un módulo (un cuadrante en el reloj de Gauss) podemos hablar de los grupos o clases refiriéndonos a uno de sus representantes. Supongamos que

elegimos un cuadrante de cuatro números, es decir, que trabajamos con el módulo 4. Sólo tendremos cuatro agrupaciones o clases de números y podemos tomar como representantes los más sencillos, que serán 0, 1, 2 y 3.

Esto significa que en vez de escribir 382 pondremos 2 (ya que 382 dividido entre 4 da como resto 2). Esto nos permite establecer la tabla de sumar como sigue:

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

Recordemos que, por ejemplo, 2 + 3 = 5, pero en el reloj de cuatro números el 5 sería equivalente al 1, o lo que es lo mismo, $5 \equiv 1 \ (mod\ 4)$.

Siguiendo los mismos criterios, la tabla de multiplicar sería:

1	2	3
2	0	2
3	2	1

En esta tabla se da la curiosa circunstancia de que dos números diferentes de cero al multiplicarlos dan cero (2 x 2 = 0). Lo mismo sucedería si construyéramos la tabla de multiplicar módulo 6 con los números 2 y 3, ya que al multiplicarlos el producto daría 6, que es lo mismo que cero, ya que $6 \equiv 0 \ (mod\ 6)$. Esto no sucede si el número que tomamos como módulo es un número primo, ya que éste no puede descomponerse en producto de factores.

Y aquí los números primos ya han hecho acto de presencia. Las congruencias se estudian en enseñanza secundaria y son, en cierta forma, un paseo agradable, pero si nos dirigimos hacia los parajes de la aritmética modular, nos volveremos a encontrar con «la piedra en el zapato», ya que los números primos son compañeros de viaje ineludibles.

La «calculadora de reloj» que había creado Gauss resultaba ser extraordinariamente potente. Podía saber que el resultado de dividir, por ejemplo, 8^{514} entre 7 daba

como resto 1 sin necesidad de hacer operaciones complicadas, ya que 8 ≡ 1 (*mod* 7), o lo que es lo mismo, 8 dividido entre 7 da como resto 1, lo que en la tabla de multiplicar quiere decir que multiplicar 8 por 8 es lo mismo que multiplicar 8 por 1: 8 x 8 = 64, que dividido entre 7 da como resto 1.

En consecuencia, multiplicar 8 por sí mismo 514 veces es como ir multiplicando por 1 el mismo número de veces; dicho de otra forma,

$$8^{514} \equiv 1 \ (mod\ 7).$$

Gauss observó en su calculadora de reloj que cuando el cuadrante tenía un número primo *p* de horas, éstas volvían a repetirse cada *p* veces, es decir, que formaban ciclos iterativos de *p* números. Gauss se reformuló entonces el pequeño teorema de Fermat en términos de su calculadora de reloj de la siguiente forma:

> «Si *p* es un número primo, entonces para cada número natural a se tiene que $a^p \equiv a$ (*mod p*)».

O bien, $a^p - a$ es múltiplo de *p*. Por ejemplo, 35 − 3 = 240, que es múltiplo de 5.

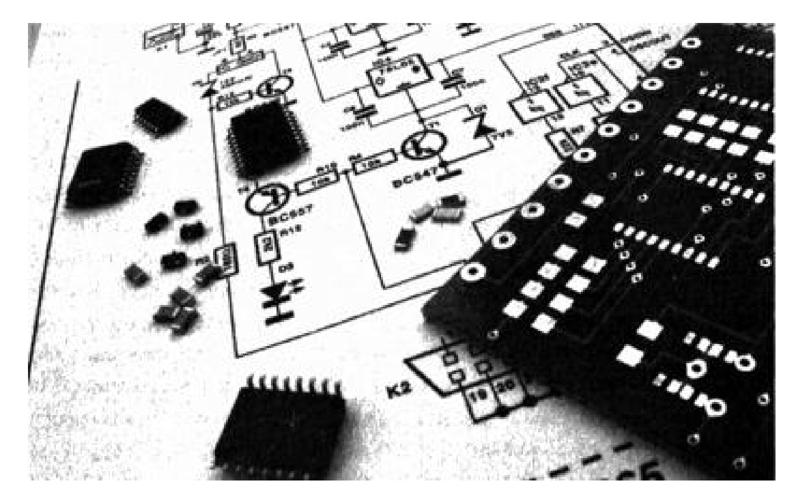
En términos del reloj de Gauss, el teorema se puede interpretar de la siguiente forma. Supongamos que queremos saber si *p* es un número primo. Construimos un reloj con un cuadrante de *p* horas, tomamos diferentes números y probamos si al elevar cualquiera de ellos a p las manecillas vuelven a marcar el mismo número. Si no es así, es que con seguridad no se trata de un número primo. Supongamos que el número que queremos investigar es el 6. Construimos un reloj de 6 horas. Ahora tomamos una hora cualquiera, por ejemplo las 2. Hacemos 2^6 = 64, que dividido entre 6 nos da de resto 4. Dicho de otro modo, las manecillas darán sucesivas vueltas al reloj hasta quedar paradas en el número 4. Sabemos seguro, según el pequeño teorema de Fermat, que el 6 no es un número primo. Se puede hacer la prueba con un número primo, por ejemplo el 7, y se comprobará que cuando lo elevamos a cualquier hora, las manecillas siempre vuelven a la misma hora. De todas maneras, hay que recordar que el teorema nos muestra una condición necesaria, pero no suficiente. Esto quiere decir que si al probar con a las manecillas

vuelven al número a, sabemos que tenemos un punto a favor para que el número p sea primo; sin embargo, la prueba no es concluyente. Cuantas más pruebas hagamos, más a favor estaremos que el número en cuestión sea primo, pero no tendremos una conclusión definitiva. Como veremos en el capítulo 7, éste es uno de los sistemas más utilizados por la informática actual para tener ciertas garantías de que un número grande es primo.

3. Números imaginarios

Al oír la expresión «números imaginarios», el profano puede llegar a pensar que se trata de una más de las muchas extravagancias de los matemáticos. Postura no del todo criticable, ya que ésta fue una opinión compartida durante mucho tiempo por varios profesionales de la comunidad matemática que querían ver fuera de sus dominios a tan exóticos números, que fueron tratados literalmente de «fantasmas». Pero estos fantasmas aparecían constantemente en la solución de ecuaciones y se hacía muy difícil ignorarlos. Se los empezó a introducir en los cálculos hasta que un día se les aceptó como soluciones de ecuaciones y adquirieron una identidad propia, pasando a ser un concepto fundamental en las matemáticas y de presencia obligada en cualquier texto de enseñanza elemental. Sería erróneo creer que su presencia se limita al mundo de la pura teoría matemática; de hecho, los números imaginarios son una herramienta básica de la física actual y tienen infinidad de aplicaciones prácticas. Si los logaritmos desempeñaron un papel decisivo en el giro que Gauss imprimió a la historia de los números primos, los números imaginarios cerrarían un ciclo con las posteriores teorías de Riemann, por lo que se hace imprescindible un pequeño viaje por el territorio de lo «imaginario» para comprender mejor la revolución que supusieron estas teorías.

Leibniz dijo en una ocasión: «El espíritu divino halló una sublime expresión en esa maravilla del análisis, ese portento del mundo ideal, ese anfibio entre el ser y el no ser que llamamos raíz imaginaria de la unidad negativa». Vamos a ver a qué se estaba refiriendo cuando hablaba de la raíz imaginaria de la unidad negativa.



Los números imaginarios tienen una aplicación práctica en la ingeniería electrónica, en la que se utilizan números reales para medir la resistencia (oposición que ofrece un cuerpo cuando pasa por él una corriente eléctrica), pero números imaginarios para la inductancia (en una bobina, la relación entre el flujo magnético y la intensidad de la corriente eléctrica) y la capacitancia (diferencia de tensión eléctrica existente entre las placas de un condensador y la carga eléctrica almacenada en él).

La raíz cuadrada de un número *a*, que se simboliza con el signo $\sqrt{a}$, es, por definición, otro número *b* tal que al elevarlo al cuadrado nos da *a*; es decir que $\sqrt{a} = b$ significa que b^2 = a. Por ejemplo:

$$\sqrt{4} = 2 \text{ porque } 2^2 = 4$$

$$\sqrt{9} = 3 \text{ porque } 3^2 = 9$$

Por otro lado, existe una regla de signos para la multiplicación y la división que se traduce en que «más por más es igual a más; más por menos (o menos por más) es igual a menos» y «menos por menos es igual a más», que escrito de forma simbólica sería:

+ x + = +

+ x − = − x + = −

$$- \times - = +$$

Esto se traduce literalmente en las operaciones entre números:

$$5 \times 2 = 10$$

$$(-5) \times 2 = -10$$

$$(-5) \times (-5) = 25$$

Según esto, el cuadrado de un número, que es el resultado de multiplicar dicho número por sí mismo, no puede dar nunca un resultado negativo, ya que si el número es positivo, «más por más», dará un resultado positivo, y si el número es negativo, «menos por menos», dará también un resultado positivo. Éste es el motivo por el que, en principio, no se puede extraer la raíz cuadrada de un número negativo. Por ejemplo, $\sqrt{-4}$ no puede ser igual a 2 ya que $2 \times 2 = 4$, ni tampoco -2, ya que $(-2) \times (-2) = 4$.

De manera que podemos afirmar que $\sqrt{1} = 1$, pero $\sqrt{-1}$ no existe. No existe como número real, pero nada nos impide definirlo como un nuevo número «imaginario», al que llamaremos *i*.

$$\sqrt{-1} = i.$$

Veamos qué sucede con este nuevo número que hemos obtenido cuando lo elevamos a diferentes potencias:

$$\sqrt{-1} = i$$

$$i^2 = (\sqrt{-1})^2 = -1$$

$$i^3 = i^2 \cdot i = (-1) \times i = -i$$

$$i^4 = i \times i^3 = i \times (-i) = -i^2 = -(-1) = 1$$

Y a partir de aquí se iría repitiendo la misma cadencia:

$$i^5 = i;$$
$$i^6 = -1;$$
$$i^7 = -i;$$
$$i^8 = 1; \ldots$$

La necesidad de hallar el valor de raíces cuadradas de números negativos apareció al intentar resolver determinadas ecuaciones de segundo grado. Se sabía que una ecuación del tipo $ax^2 + bx + c$ tenía dos soluciones que venían dadas por la fórmula:

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Pero la solución del problema quedaba colapsada cuando la cantidad que figuraba dentro de la raíz era negativa.

En uno de los problemas que aparece en la obra A*rs Magna* de Girolamo Cardano (1501-1576), publicada en 1545, aparece el siguiente problema: «Dividir 10 en dos partes cuyo producto sea 40». Si llamamos x e y a esas dos partes, se tiene que:

$$x + y = 10$$
$$x\,x\,y = 40$$

Aislando $y = 10 - x$ y sustituyendo en la segunda ecuación se llega a la siguiente conclusión:

$$x(10 - x) = 10x - x^2 = 40$$

y pasándolo todo al segundo miembro se tiene la ecuación de segundo grado

$$x^2 - 10x - 40 = 0$$

cuyas soluciones serán:

$$x = \frac{10 \pm \sqrt{100 - 160}}{20} = \frac{10 \pm \sqrt{-60}}{20} = 5 \pm \sqrt{-15}$$

Cardano estudió los dos números que ha obtenido como solución,

$$5 + \sqrt{-15} \text{ y } 5 - \sqrt{-15}.$$

Consciente de que son números complejos, observa que la suma es 10 y el producto, 40, y que, por tanto, son, a pesar de «las torturas mentales que ellos implican», soluciones de la ecuación propuesta.

Estas raíces «complejas» aparecían con frecuencia como soluciones en multitud de problemas (recordemos que cuando se habla de las raíces de una ecuación se está haciendo referencia a las posibles soluciones de la misma). Estaban ahí e incomodaban a los matemáticos, que en ningún caso las consideraban como números. El mismo Descartes afirmaba refiriéndose a ellas: «Ni las raíces verdaderas ni las falsas son siempre reales, a veces son imaginarias», con lo que acuñó uno de los términos que se utilizarían desde entonces para referirse a este tipo de raíces: «imaginarias».

Un número imaginario como $\sqrt{-4}$ se puede escribir también de la forma $\sqrt{4} \times \sqrt{-1} = 2 \times \sqrt{-1}$ y ya que hemos llamado i a la raíz cuadrada de -1, podemos poner: $\sqrt{-4} = 2i$

De modo que todo número complejo se puede escribir de la forma a + bi, llamada forma binómica de los números complejos, en la que «a» es la parte real del mismo y «b», la imaginaria. Por ejemplo, el número $2 + \sqrt{-9}$ se puede poner como $2 + 3i$, siendo 2 la parte real y 3, la imaginaria. Cuando un número complejo no tiene parte real, como $2i$, se dice que es imaginario puro.

La suma y la resta de números complejos es muy sencilla, y se lleva a cabo de la siguiente forma: «La suma de dos números complejos es otro número complejo cuya parte real es la suma de las partes reales de cada uno de los números y cuya parte imaginaria es la suma correspondiente de las partes imaginarias». Por ejemplo:

$$(3 + 2i) + (8 - 3i) = (3 + 8) + (2 - 3)\, i = 11 - i.$$

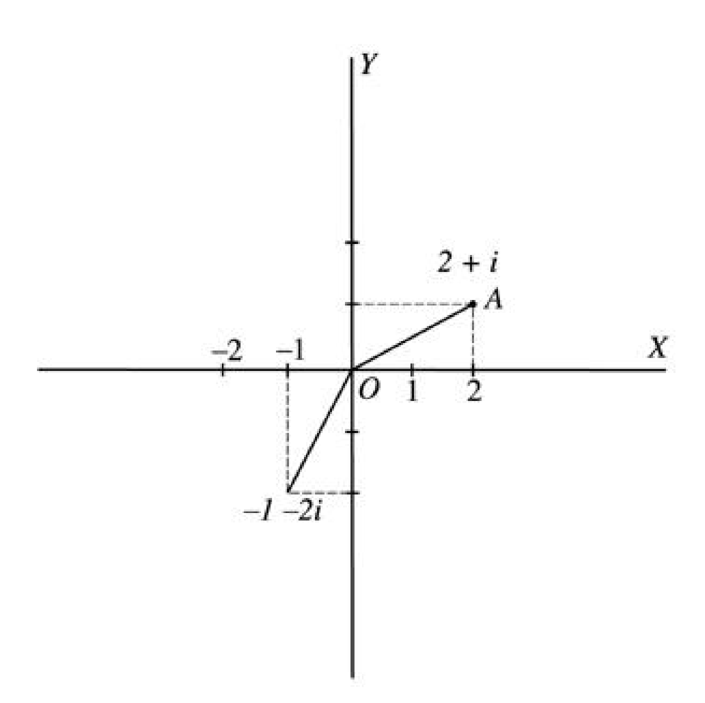
Para la resta, se sigue una regla análoga. Para la multiplicación, se pueden poner uno debajo del otro y efectuar una multiplicación normal y corriente, como lo haríamos con números cualesquiera.

En términos algebraicos, los números complejos se podían manejar sin problemas, pero no se tenía una imagen clara de ellos, como la que se tiene de los números reales, a los que se puede representar a lo largo de una recta, para lo cual basta con asignar un punto de referencia al que llamamos «cero», situar a la derecha de éste los números positivos y a la izquierda, los negativos; con esto es suficiente. Pero los números complejos venían representados por una pareja de números, y esto, de alguna u otra forma, suponía un cambio de dimensión en el espacio geométrico. La representación geométrica de los números complejos ha tenido una larga trayectoria histórica. Varios matemáticos, entre los que cabría destacar a Euler, Abraham De Moivre o Alexandre-Théophile Vandermonde, ya se habían planteado la posibilidad de imaginar un número complejo $x + yi$ como un punto del plano de coordenadas (x, y). Pero fue gracias al trabajo de Jean-Robert Argand (1768-1822), un contable aficionado a las matemáticas cuya única aportación fue un breve estudio sobre la representación geométrica de números complejos, así como a los planteamientos de Gauss, quien determinó su naturaleza geométrica, que los números complejos adquirieron su forma definitiva tal y como la conocemos hoy. De hecho, Gauss fue quien introdujo el símbolo i para representar $\sqrt{-1}$ y era de la opinión de que a 1, -1, $\sqrt{-1}$ no se los debía llamar unidades positiva, negativa e imaginaria, sino directa, inversa y lateral. De esta forma, la aceptación de los números imaginarios habría sido más rápida, al despojarles de su aire de

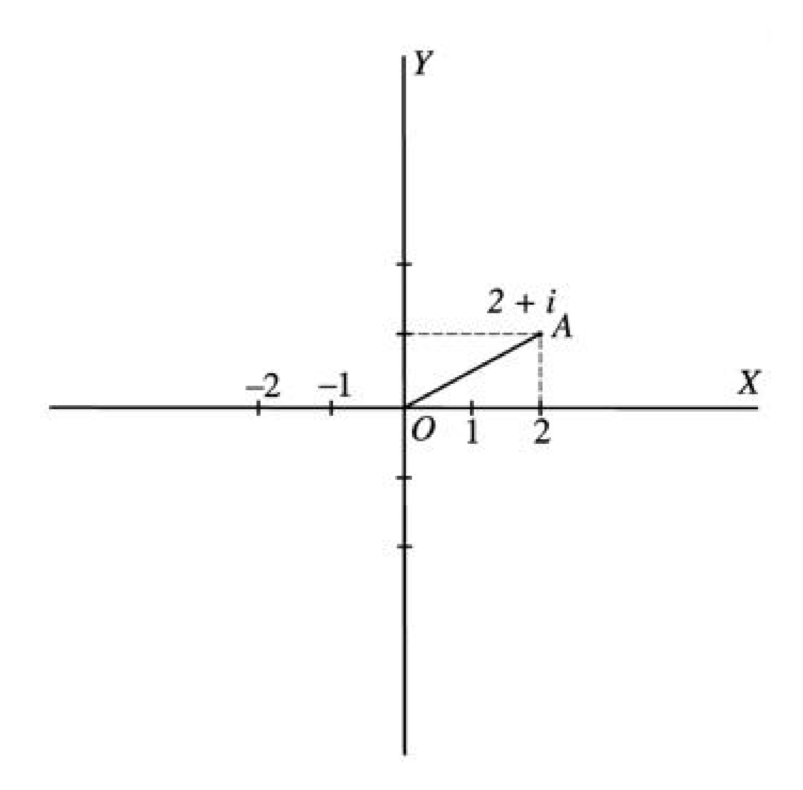
misterio. También fue quien, siguiendo el mismo criterio, introdujo el término «número complejo» para sustituir al de «número imaginario».

La representación de los números complejos es sencilla y se lleva a cabo de la siguiente forma: tomemos en el plano unos ejes de coordenadas rectangulares. Al eje OX lo llamamos eje real, que es donde situaremos la parte real del número complejo, a la derecha si es positivo y a la izquierda si es negativo. Al eje vertical OY lo llamaremos eje imaginario, y en él localizaremos la parte imaginaria del número complejo, en la parte superior si es positivo y en la inferior si es negativo.

Así, para representar el número complejo 2 + *i* haremos



Tomaremos dos unidades en la parte positiva del eje OX y una unidad en la parte superior del eje OY. La distancia OA la podemos calcular aplicando el teorema de Pitágoras, siendo $(OA)^2 = 1^2 + 2^2 = 1 + 4 = 5$, con lo que $OA = \sqrt{5}$, cantidad que recibe el nombre de *módulo* del número complejo.



El hecho de poder representar de manera gráfica los números complejos supuso un gran paso porque significaba que iban a poder incluirse en el análisis matemático de funciones en las que la variable pudiera venir representada por un número complejo.

Funciones con números complejos

Desde que Cardano hiciera sus primeros cálculos con los números imaginarios hasta principios del siglo XVIII, los matemáticos trataron de evitar cualquier encuentro con unos números de cuya existencia dudaban seriamente. Matemáticos de la talla de Euler, Wallis o D'Alembert se enfrentaron a ellos con mayor o menor éxito. Los números complejos empezaron a mostrarse útiles en determinados contextos, especialmente en los pasos intermedios de algunas demostraciones. Gauss fue uno de los primeros en tratar con ellos «de tú a tú» y estableció incluso una forma de representarlos, pero hasta el siglo XIX no se implantarían de forma casi definitiva gracias a la aparición en escena, de la mano de Riemann, de las funciones complejas, funciones f(x) en las que la variable x es un número

complejo.

4. Una dimensión más

La observación, por un ojo experto, de la representación gráfica de una función puede proporcionar niveles de información insospechados. En este sentido, y si no fuera por su exagerado nivel de concreción, se la podría considerar como una obra de arte. Como afirmaba Lord Kelvin: «Una simple curva, trazada a la manera de la curva de los precios del algodón, describe todo lo que el oído puede escuchar como resultado de las más complicadas composiciones musicales. En mi opinión, esto es una maravillosa prueba de la potencia de la matemática».

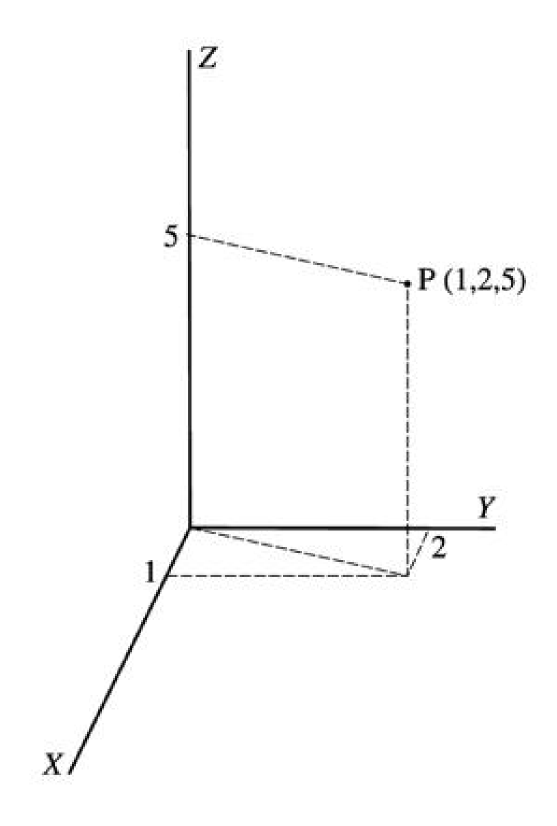
Ya vimos en el capítulo III que es posible representar funciones en las que a cada número real se le asigne otro número real. Mediante un mecanismo similar pueden representarse funciones que asignen un número real a cada par de números reales Por ejemplo:

$$(x, y) \to x^2 + y^2.$$

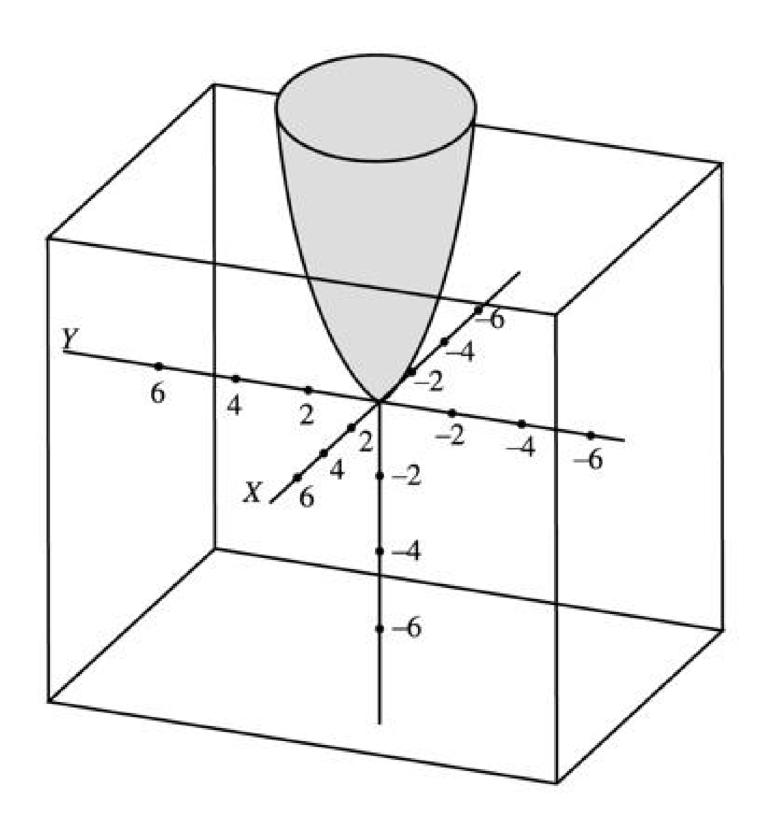
Para la que la tabla correspondiente sería

(x, y)	$x^2 + y^2$
(1, 1)	2
(1, 2)	5
(3, 5)	34
(2, 3)	13
...	...

Para la representación de una función como ésta es preciso recurrir a un espacio tridimensional donde, por ejemplo, la imagen del punto (1, 2, 5), que se encuentra en el plano, está situada a una altura de 5 en la dirección del eje perpendicular a dicho plano.



Y una representación de la función $f(x, y) = x^2 + y^2$ sería:



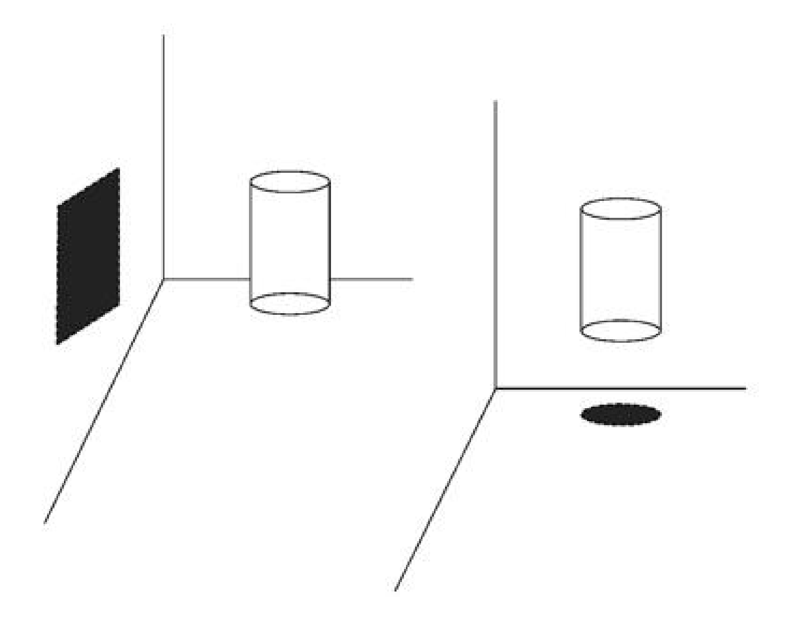
En el siglo la teoría de funciones se había desarrollado lo suficiente como para abordar este tipo de gráficas de manera bastante satisfactoria. Sin embargo, el nuevo problema que iba a aparecer en el horizonte era la posibilidad de introducir en las variables los números complejos, un paso que habría de resultar decisivo en la investigación de los números primos.

Gauss ya había introducido las funciones de variable compleja diseñando un espacio tridimensional donde poder representarlas. Como veremos en el próximo capítulo, Riemann dio un paso más allá y definió lo que habían de ser las funciones complejas de variable compleja. En las representaciones espaciales que hemos visto hasta ahora teníamos que la imagen de dos números daba como resultado otro número. Partíamos de una posición en el plano y la imagen la calculábamos en un tercer eje, lo que implica trabajar en un espacio de tres dimensiones. Pero ahora lo que nos planteamos es que, partiendo de un punto con dos coordenadas, la imagen también sea un punto con dos coordenadas. Dicho de otra forma, nos falta una dimensión para poder hacer la representación gráfica, ya que una función de este tipo sólo puede representarse en un espacio de cuatro dimensiones. Visualizar una gráfica en cuatro dimensiones es algo a lo que debemos renunciar fuera del ámbito de la ciencia ficción. Por consiguiente, no queda más remedio que utilizar algunos trucos que nos den una idea de la forma que puede tener el objeto en cuestión.

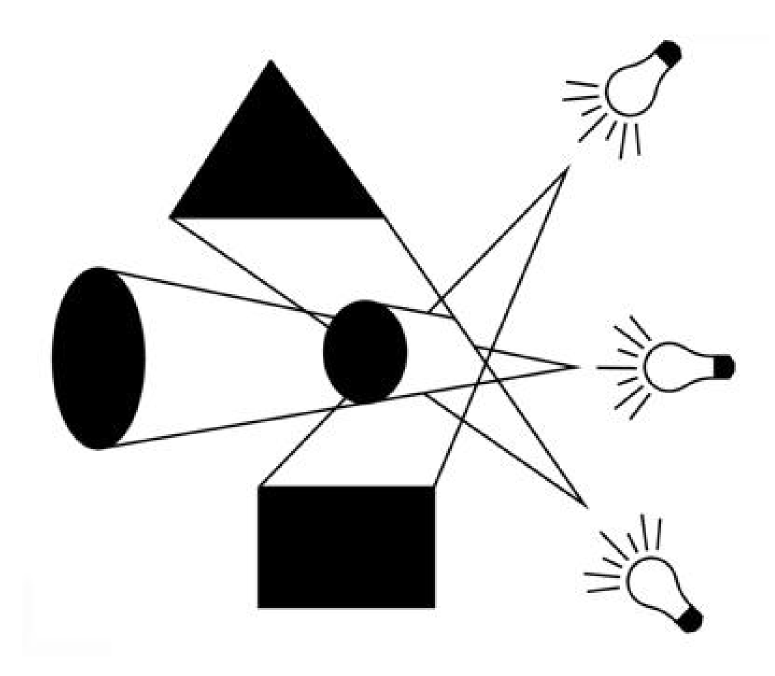
Una posibilidad es estudiar sus proyecciones sobre el espacio de tres dimensiones, algo así como si examináramos sus sombras. Para comprenderlo, es muy útil imaginar que nosotros nos movemos en un espacio de dos dimensiones, que somos seres completamente planos y que intentamos averiguar la forma que tiene un objeto que ocupa un espacio de tres dimensiones. Una sombra viene a ser la proyección sobre un plano de un objeto que está iluminado por un foco.

Quizá la sombra proyectada sobre un plano sea insuficiente y necesitemos dos o tres proyecciones más. Por ejemplo, un cilindro que se encuentra suspendido en el aire en medio de una habitación podría proyectar sobre una de las paredes la figura de un rectángulo, lo que podría darnos una idea equivocada de la figura que estamos estudiando. Podríamos pensar que se trata de un paralelepípedo, que en realidad proyectaría el mismo tipo de sombra. Si observáramos, además, la sombra que proyecta sobre el suelo, nos encontraríamos con que ésta es un círculo, lo que

inmediatamente cambiaría nuestra primera idea y nos empezaríamos a aproximar más a la realidad del cilindro. El problema es que, como seres de dos dimensiones que seríamos, nunca habríamos visto un cilindro en tres dimensiones.



Por otro lado, las sombras pueden resultar muy engañosas o ser de muy difícil interpretación. Pensemos, por ejemplo, en un objeto que al iluminarlo por el lado derecho produce en la pared la sombra de un círculo. En cambio, cuando lo iluminamos desde abajo la sombra es un triángulo, y al hacerlo desde arriba nos proyecta un cuadrado. ¿Existe algún objeto tridimensional con estas características? Si existiera, podría tratarse de un corcho muy especial que sirviera para tapar botellas de cuello circular, triangular o cuadrado.



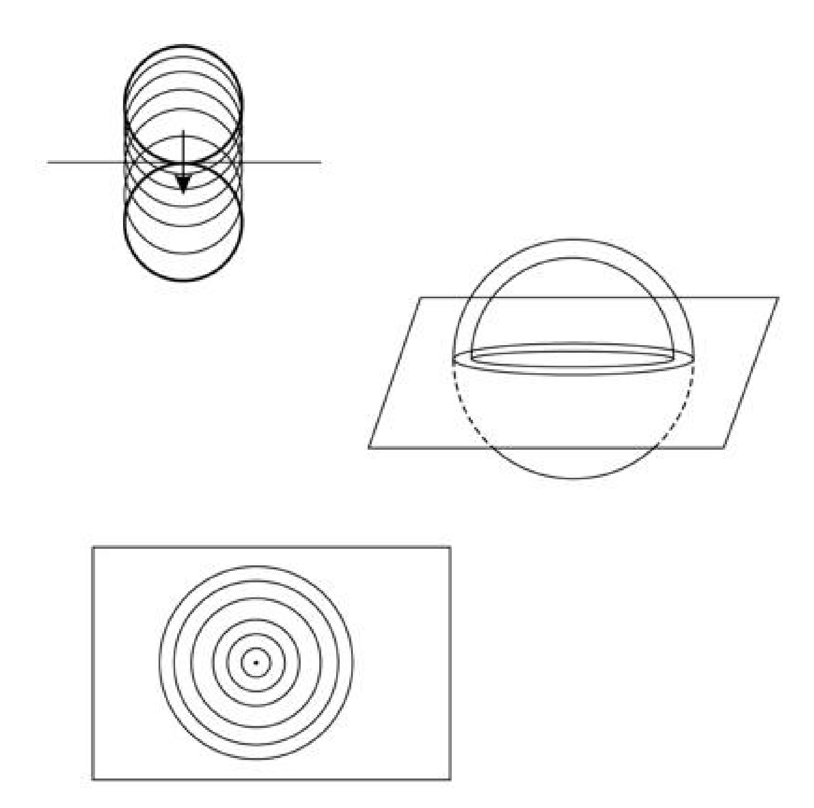
La pregunta que se plantea ahora es ¿existe alguna relación entre las diferentes sombras de un mismo objeto que nos pueda definir la forma tridimensional del objeto? La respuesta a esta difícil pregunta la obtuvo en 1986 Ken Falconer, profesor de matemáticas de la Universidad de St. Andrews, como consecuencia de un teorema. Y la respuesta es no; en general, no existe ninguna relación de este tipo.

¿Qué hacer entonces cuando se quiere saber cómo es una figura ubicada en un espacio de cuatro dimensiones? La forma exacta que tiene no la podremos saber nunca, entre otras cosas porque aunque tuviéramos la posibilidad de representarla, no tendríamos la facultad o los sentidos necesarios para verla. Lo que sí hay son técnicas analíticas que nos permiten conocer ciertas características geométricas de la figura en cuestión.

Volviendo al ejemplo en el que nos convertíamos en seres planos, las técnicas empleadas se asemejan a las que utilizaríamos para saber cómo es una esfera si fuéramos seres de dos dimensiones. El truco consiste en obtener cortes transversales de la esfera en su intersección con el plano en el que nos encontramos «viviendo» y observar detenidamente las figuras resultantes.

Cuando la esfera es tangente al plano, lo primero que veríamos es un punto. A continuación irían apareciendo una serie de círculos concéntricos que irían

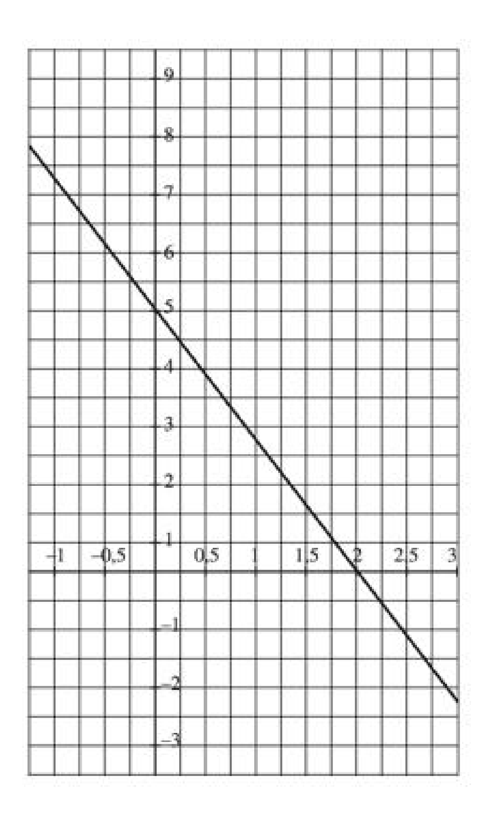
aumentando de tamaño, para luego empezar a disminuir y convertirse, cuando la esfera ha acabado de cruzar totalmente el plano, otra vez en un punto.



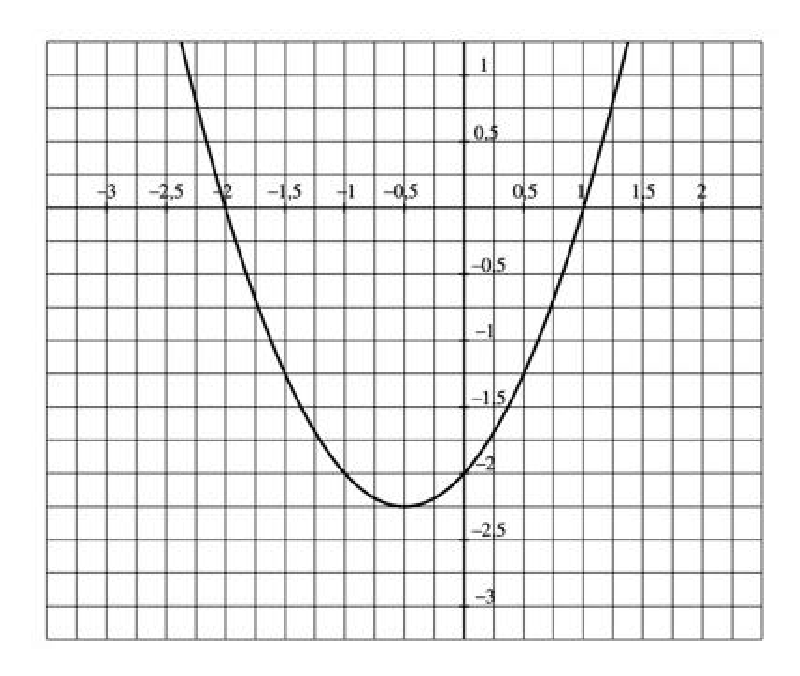
Cabe señalar que, en este ejemplo, podemos tener una perspectiva clara de la situación porque tenemos el privilegio de adoptar un punto de vista tridimensional, algo que nos está vedado cuando debemos manejarnos en un espacio de cuatro dimensiones. Pero lo relevante del ejemplo es que sí podemos saber lo que sucede en el espacio de la intersección, en el corte de la figura con el plano, y esto es tan importante porque tiene una estrecha relación con lo que se denominan los ceros de una función.

Una ecuación como $-5x/2 + 5$ puede convertirse en una función haciendo simplemente $y = -5x/2 + 5$

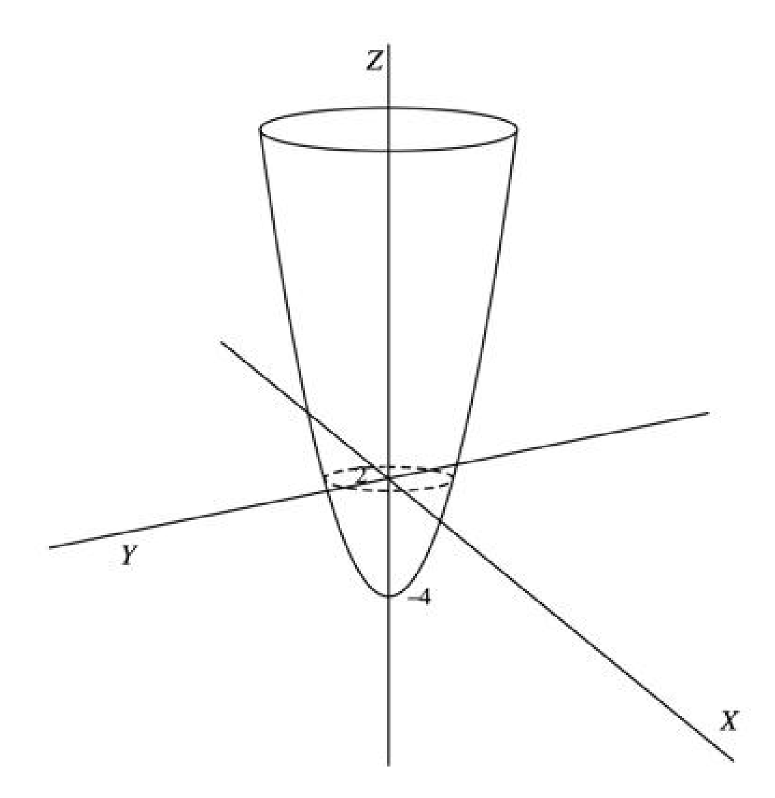
Si la representamos, tendremos una recta. La intersección de dicha recta con el eje horizontal ($x = 2$) es precisamente la solución de la ecuación.



De forma análoga, si tenemos la ecuación de segundo grado $x^2 + x - 2 = 0$ y representamos la función $f(x) = x^2 + x - 2$, observaremos que la intersección de dicha función con el eje OX nos da dos puntos que son precisamente las soluciones $x = 1$ y $x = -2$ de la ecuación.



Si aumentamos el problema a tres dimensiones, la ecuación $x^2 + y^2 - 4 = 0$ puede venir representada por una función como $f(x, y) = x^2 + y^2 - 4$, que es una paraboloide cuya intersección con el plano XY nos da una circunferencia de radio 2, tal como se observa en la figura siguiente. Todos los puntos de dicha circunferencia son soluciones de la ecuación propuesta.



De manera que cuando empleemos el truco ilustrado antes para «ver» cómo es una figura de cuatro dimensiones, lo que interesa en realidad es tener una idea precisa de la intersección de dicha figura cuatridimensional en el espacio de tres dimensiones. Esto no nos dará una idea precisa de la forma de la figura, que por otro lado sabemos que nunca podremos tener, pero sí de las soluciones que plantea la ecuación correspondiente. Y éste era, como veremos en el próximo capítulo, el propósito de Riemann cuando analizó la famosa función zeta, que iba a intentar imponer un ritmo al conjunto de los números primos.

Legado cultural

Si dijéramos que «una función es una cantidad compuesta de cualquier manera a partir de una variable y constantes arbitrarias», tal definición no pasaría un examen de matemáticas elementales, ya que denotaría que su autor no acaba de tener claro el concepto de función. Sin embargo, procede textualmente nada menos que de Johann Bernoulli, uno de los matemáticos más importantes del siglo XVIII. Y es que no fue nada sencillo llegar a establecer el concepto de función, algo que actualmente puede conocer cualquier alumno de enseñanza secundaria; este hecho demuestra la extraordinaria solidez que tienen las matemáticas como legado cultural.

Capítulo 6
Las dos caras de una moneda

Contenido:

1. *Bernhard Riemann*
2. *A propósito de Ramanujan: sobre el pensamiento*

El alemán Bernhard Riemann (1826-1866) y el indio Srinivasa Ramanujan (1887-1920) representan el paradigma del rigor matemático el primero y de la imaginación en estado puro el segundo. Ambos se enfrentaron a los números primos y cosecharon éxitos y fracasos. En cualquier caso, su vida y su trabajo son un exponente extraordinario del pensamiento matemático.

1. Bernhard Riemann

Riemann es el batería que consigue establecer un ritmo con el que todo el público (los números primos) se pone a batir palmas al unísono. Lo que sucede es que se trata de un ritmo muy complicado. La divulgación científica, especialmente la de matemáticas, resulta difícil cuando nos adentramos en según qué territorios. El divulgador viene a ser algo así como un guía de montaña.

Cuando se trata de senderismo sólo hay que ocuparse de no perder la orientación, pero cuando se empiezan a subir montañas, la cosa cambia. Hay excursiones que requieren de cierto esfuerzo, por lo que hay que ir con paso tranquilo para que la ascensión no resulte excesivamente fatigosa, aunque llega un punto en el que los excursionistas necesitan cierta preparación y medios técnicos adecuados. No es lo mismo ascender a un pico de 2.000 m que a uno de 4.000. Con Riemann empezamos los «cuatromiles».

Georg Friedrich Bernhard Riemann nació en Breselenz, en el reino de Hanover. Quizá debido a su extrema timidez y a su temor, casi patológico, a hablar en público, no siguió las directrices que le había marcado su padre, pastor luterano, para encaminarlo a la predicación. Friedrich Constantin Schmalfuss, director del instituto en el que estudiaba el joven Riemann, le permitió llevarse a su casa un

libro de su biblioteca particular, la Teoría de números de Legendre, un tratado de matemáticas de gran complejidad. Riemann lo leyó de cabo a rabo en apenas una semana y se lo devolvió diciéndole que le había parecido muy interesante. No se trataba de un farol: de ese compendio, Riemann extraería años más tarde los elementos necesarios para elaborar su teoría sobre los números primos, dando lugar a una de las conjeturas más famosas de la historia de las matemáticas

A los 19 años, Riemann asistió, en Universidad de Gotinga, a las conferencias matemáticas de Moritz Stern; fue entonces cuando tuvo su primer contacto con los trabajos de Gauss. Un año más tarde se matriculó en Matemáticas en la Universidad de Berlín, donde tuvo como profesores a Peter Gustav Lejeune Dirichlet, Carl Jacobi, Jakob Steiner y Ferdinand Eisenstein.



Bernhard Riemann.

Gracias a la intensa relación que mantuvo con este último nació una de las teorías matemáticas más importantes del siglo XIX, la «teoría de funciones de variable compleja», herramienta fundamental que le permitiría establecer su hipótesis en relación con los números primos.

Tesis doctoral

«Creo que he mejorado mis perspectivas con mi disertación. Espero también aprender a escribir más rápidamente y con mayor fluidez, especialmente si frecuento la sociedad y si tengo probabilidades de pronunciar conferencias; por tanto, tengo buen ánimo». Con estas palabras, escritas en una carta a su padre, Riemann se refería a la lectura de su tesis doctoral que, a los 25 años, presentó en la Universidad de Gotinga, cuyo título era Fundamentos para una teoría general de las funciones de una variable compleja. Su lectura despertó el entusiasmo de Gauss, una de las figuras míticas de la matemática de la época.

La función zeta

Como hemos visto en el capítulo 3, Euler había definido una función basada en la serie armónica y cuya expresión es

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \cdots + \frac{1}{n^x} \ldots = \sum_{n=1}^{\infty} \frac{1}{n^x}$$

El matemático suizo ya había comprobado que la suma era infinita si x tomaba valores iguales o inferiores a 1. Llegó a calcular un par de valores, para x = 2 y x = 4:

$$\zeta(2) = \frac{\pi^2}{6}; \quad \zeta(4) = \frac{\pi^2}{90}$$

Vimos también que el mismo Euler estableció una relación entre esta función y los números primos (el llamado producto de Euler), relación que luego le sirvió tanto a él como a otros matemáticos para demostrar la infinitud de los números primos, que ya en su momento había demostrado Euclides mediante técnicas elementales.

Por otro lado, Gauss había conjeturado, pero no demostrado, que para valores grandes de x,

$$\pi(x) = \frac{x}{\ln x}$$

Recordemos que π (x) es el número de primos menores que x.

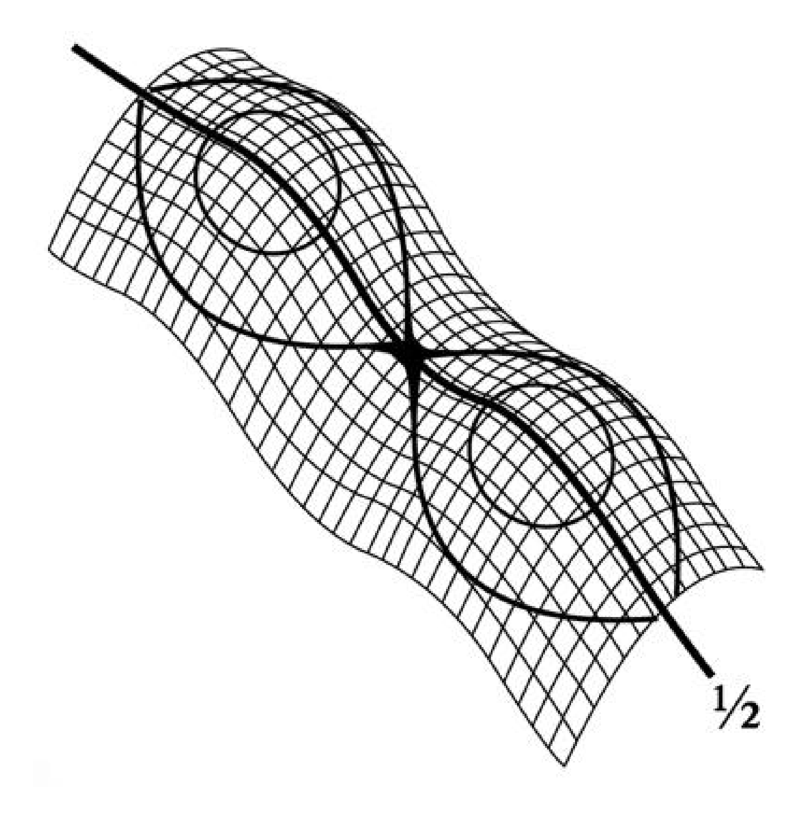
Riemann se propuso estudiar la conjetura de Gauss valiéndose de la función zeta de Euler y pensó que el camino más fructífero sería ampliar dicha función al dominio de los números complejos. Para ello ideó un sistema llamado «prolongación analítica» (en rigor, esta extensión analítica es a la que debemos referirnos cuando hablamos de la función zeta de Riemann):

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x} = \prod_{p} \frac{1}{1 - p^{-x}}$$

La segunda parte de la igualdad, un producto infinito extendido a todos los números primos *p*, hace referencia al producto de Euler y relaciona la función zeta con los números primos (recordemos que este producto se obtenía como consecuencia directa del teorema fundamental de la aritmética de Euclides).

Ya hemos visto que Gauss introdujo las funciones de variable compleja diseñando un espacio tridimensional en el que podían ser representadas. Riemann da un paso más allá y define lo que han de ser las funciones complejas de variable compleja. El problema era que ahora éstas no iban a poder visualizarse, ya que para ello requieren de un espacio de cuatro dimensiones.

Utilizando sofisticadas técnicas, similares a las que apuntamos en el capítulo anterior, Riemann obtuvo una imagen tridimensional de los ceros de la función zeta, un paisaje en el que aparecen valles y montañas distribuidos con cierta regularidad.



En esta función hay dos clases de ceros, valores que, al sustituirlos en la función, dan como resultado el valor cero. Unos son los enteros pares negativos, x = −2, x = −4, x = −6,... que son las llamadas «soluciones triviales». Los demás ceros no tienen nada de trivial, y su cálculo resulta extremadamente difícil: son infinitos y se encuentran todos en la denominada «banda crítica», aquellos cuyos valores reales se sitúan entre 0 y 1 ($0 \leq Re(x) \leq 1$), una franja del paisaje que está íntimamente relacionada con los números primos. Fue en este escenario concreto donde dos matemáticos, Jacques Hadamard y Charles de la Vallée Poussin, demostraron, en 1896 y de forma independiente, el «teorema de los números primos» que había sido enunciado por Gauss.

En una nota algo informal y sin ningún tipo de demostración, Riemann adelantó que todos los ceros no triviales de la función zeta eran de la forma $1/2 + iy$, que era tanto como decir que se encontraban en la recta $x = 1/2$ Esta afirmación constituye lo que se conoce como conjetura o hipótesis de Riemann, que dice exactamente:

«La parte real de todo cero no trivial de la función zeta es 1/2».

Si la hipótesis es cierta, significa que todos los números primos se distribuyen de una forma regular, o, mejor dicho, de la forma más regular posible. Esto último puede interpretarse, mediante una fiel analogía, de la siguiente forma: imaginemos una función que represente el análisis de un sonido, una serie de curvas sinusoidales que reflejan un concierto de violín. Para explicarlo con mayor claridad, supongamos que se trata de un solo de violín. Junto a una serie de crestas y valles bien definidos, pueden aparecer otras figuras no tan bien definidas y que en cierta forma «rompan la armonía» de la gráfica. Esto es lo que técnicamente se llama «ruido aleatorio», que se debe a muy diferentes causas (sonidos electrostáticos, ruido ambiental esporádico, etc.). Pues bien, la hipótesis de Riemann viene afirmar que las posibles irregularidades que aparecen en la distribución de los Números primos proceden de ruido aleatorio, lo cual significaría que los números primos siguen una pauta en su distribución y que ésta no es debida al puro azar, en este sentido ya hemos dicho que Riemann había conseguido imponer un ritmo a la alocada banda.

Puede intentarlo usted

Si decide ampliar sus conocimientos sobre funciones de variable compleja y series, temas sobre los que existe una abundante bibliografía, puede intentar demostrar la hipótesis de Riemann. En el caso de. que lo consiga, el Clay Mathematics Institute le premiará con la nada despreciable cantidad de un millón de dólares en efectivo, sin importar su edad, sexo o profesión. De todas maneras, seguramente tardará un tiempo en recibir el premio, ya que primero es preciso constatar que la demostración es correcta. En junio de 2004, Louis de Branges de Bourcia, matemático de la Purdue University West Lafayette, Indiana, aseguró haberlo conseguido, aunque la demostración no fue aceptada; lo mismo sucedió en 2008.



En 1914, los matemáticos británicos Godfrey Harold Hardy (1877-1947) y John Edensor Littlewood (1885-1977) demostraron que existían infinitos ceros sobre a recta, lo que no demuestra la hipótesis de Riemann, pero en todo caso acrecienta la opinión, muy generalizada entre la comunidad matemática, de que dicha hipótesis es cierta. Hay quien puede pensar que si hay infinitos ceros sobre la recta crítica ya deben de estar todos, pero ése es un pensamiento que indica ciertos desconocimientos sobre el concepto de infinito (un mundo lleno de paradojas) ya que, además, es posible que hubiera infinitos ceros que no estuvieran sobre dicha recta. Actualmente ya se llevan computados unos diez millones de ceros no triviales que se encuentran en la recta crítica.

En una ocasión le preguntaron al eminente matemático alemán David Hilbert cuál sería la primera información que pediría en un congreso de matemáticos que se celebrara cien años después de su muerte, a lo que contestó: «Preguntaría si la conjetura de Riemann ya ha sido demostrada». A día de hoy, nadie lo ha conseguido.

Las paradojas del infinito: el Hotel de Hilbert

El hotel de Hilbert es un hotel imaginario que dispone de infinitas habitaciones. Su gerente se jacta de que nunca deja colgado a un cliente. El caso es que una noche, en la que todas las habitaciones del hotel están ocupadas, se presenta de improviso un nuevo cliente. El conserje acude al gerente comunicándole la imposibilidad de alojarlo, a lo que éste responde que les pida a los huéspedes que ya están alojados que se cambien de habitación y pasen a ocupar la siguiente, de manera que el que ocupa la Nº 1 pase a la 2, el de la 2 a la 3, etc. Una vez realizada la operación queda libre la habitación Nº 1, que es la que le dan al recién llegado. Pero, a medianoche, el conserje acude de nuevo al gerente. Esta vez su rostro refleja cierta desesperación. Se acaba de presentar un grupo de infinitos matemáticos que acuden a un congreso, « ¡Esta vez nos va a ser imposible alojarlos a todos!». Después de reflexionar un instante, el gerente propone lo siguiente: «Deberemos pedirles un nuevo favor a nuestros clientes. Cada uno de ellos debe multiplicar por dos el número de su habitación y trasladarse a la que tenga por número el resultado de la operación». O sea, que quien esté en la 4 pasa a la 8, el de la 23 a la 46, el de la 352 a la 704 y así sucesivamente. Una vez realizada la operación, en el hotel quedan libres todas las habitaciones que tienen número impar, que como son en número infinito, permite alojar a todos los miembros del congreso.



2. A propósito de Ramanujan: sobre el pensamiento matemático

Henri Poincaré (1854-1912) afirmaba que el trabajo matemático se desarrolla en tres etapas.

La primera consiste en un análisis depurado que ponga de manifiesto las dificultades del problema y de los diferentes enfoques necesarios para abordarlo, de las herramientas de que se dispone, lo que supone una revisión a fondo de sus conocimientos.

La siguiente la define como una etapa de aparente abandono. Se deja de pensar en el problema o, por lo menos, se deja de pensar de una manera determinada para que la mente se adentre en ese misterioso territorio de la inconsciencia, en el que la actividad creadora sigue sus propias pautas. Es el territorio de la imprecisión, de la inexactitud y el vagabundeo intelectual.

El resultado de este proceso inconsciente puede aparecer en cualquier momento, por sorpresa y ligado a acontecimientos que aparentemente nada tengan que ver con el objeto de la investigación. Es el momento que relata el matemático irlandés *sir* William Hamilton (1805-1865) cuando, el 6 de octubre de 1843, paseando con

su mujer por los alrededores de Dublín, se detuvo en seco como si hubiera pisado un cable de alta tensión.



Henri Poincaré fue un hombre de ciencia y destacado en todos los ámbitos de las matemáticas.

Según sus propias palabras: *«... Ahí cerré el circuito galvánico de mi pensamiento y las chispas que cayeron fueron las ecuaciones fundamentales entre i, j, k,...»*. Hamilton se refería a que no eran tres, sino cuatro los números que hacían falta para describir el comportamiento espacial de un número hipercomplejo. Es el momento mágico en el que el investigador tiene la sensación de que repentinamente se ha encendido una luz en una habitación en la que nunca había estado antes. Poincaré analiza entonces el proceso de selección que lleva a cabo el inconsciente para traernos al consciente algunas ideas y rechazar otras, llegando a la conclusión de que, siendo incapaz de dilucidar la veracidad o falsedad de dichas ideas, su único criterio de selección está basado en la belleza matemática.

A partir de este punto, la tercera etapa es la de la plena consciencia en la que el matemático somete a un severo juicio las ideas, aceptando unas y rechazando

otras. Puede haber uno o varios retornos a la segunda etapa hasta que finalmente, si el problema se ha resuelto, se somete a las reglas de juego que impone el formalismo matemático y se le da la forma definitiva a la solución.

Todas las etapas son importantes para el cumplimiento de un descubrimiento matemático, pero, para muchos, la segunda es la más fascinante porque es la del «vuelo Ubre» de la mente que no se encuentra sujeta a los rigores del pensamiento consciente. Jacques Hadamard dedicó una de sus obras, *Psicología de la invención en el campo matemático* (1945), a estudiar el papel que desempeña el inconsciente en la actividad creativa, centrándose especialmente en la mente matemática. En dicha obra describe la creación matemática como un proceso que se inicia con una elección deliberada de los aspectos más importantes del problema, obteniendo, en la mayoría de los casos, resultados en absoluto concluyentes. Hadamard creía que este periodo debía ir seguido de un «descanso», un alejamiento del problema, tras el cual aparecían inesperadamente momentos de inspiración, de iluminación, resultado de procesos no advertidos conscientemente por el investigador.

Por último, llegaba el estadio que llamaba «de precisión», en el que el formalismo hacía acto de presencia y en el que los resultados eran ordenados de forma secuencial. Consideraba que la intervención del inconsciente a lo largo de todo el proceso creativo era crucial, especialmente en el periodo de descanso.

Las conclusiones de Hadamard coinciden con las de Poincaré, sólo que este último hace una mayor incidencia en los periodos de descanso. Aquí hay que entender, literalmente, que en dicho periodo suelen incluirse las etapas del sueño. Hay diversos testimonios en la historia de la ciencia, y de la creatividad matemática en particular, de que numerosas «ideas clave» en los procesos de investigación tuvieron lugar durante el sueño. Es curioso que la mayoría de las veces no se hace referencia a un sueño concreto en el que el autor esté trabajando en su investigación, sino al hecho de que al despertar encuentra la solución a un problema al que había dedicado un intenso trabajo durante la vigilia previa. El mismo Dirichlet, por poner un ejemplo, decía que dormía con *las Disquisitiones Arithmeticae* de Gauss debajo de la almohada porque sabía que durante el sueño tenía lugar un misterioso proceso, que él no controlaba, gracias al cual al día

siguiente conseguía desentrañar las partes oscuras del texto que durante la vigilia se había visto incapaz de descifrar.

Todo esto también forma parte del mundo mágico al que hemos hecho referencia en capítulos anteriores. Hay que insistir una vez más en que no se trata de magia en el sentido coloquial de la palabra. En su sentido tradicional los rituales o ceremoniales mágicos tienen por objeto que «alguien» o «algo» nos revele verdades ocultas. En el sentido que aquí queremos darle se trata de que un ritual, una creencia o, mejor aún, la actividad onírica por sí misma, deje a la mente en un estado especial en el que, como decíamos antes, liberada de ciertas sujeciones, pueda ejercer otro tipo de pensamiento. Es como si se cambiara el dial de un receptor que en una determinada banda

de frecuencias puede oír cosas diferentes, aunque el emisor sea siempre el mismo. Almacenamos la información en el cerebro, pero puede haber muchas maneras diferentes de gestionarla. En este escenario mental que estamos planteando hubo un matemático que se puede considerar paradigmático. De las tres etapas creativas que definían Poincaré o Hadamard, se podría afirmar que Ramanujan se movía a sus anchas en la segunda y que tenía serias dificultades en la tercera.

Debido a las circunstancias en que se educó, matemáticamente hablando, carecía de los recursos que una formación académica posibilita para el formalismo que toda demostración requiere.

Dicho en otras palabras, Ramanujan podía «ver» resultados, pero tenía serias dificultades para demostrarlos, por lo menos para demostrarlos en el marco que la comunidad matemática consideraba el adecuado. Ramanujan no sería leyenda si su historia y sus trabajos matemáticos no estuvieran sobradamente documentados. Sin educación ni recursos económicos, acabó siendo uno de los matemáticos más importantes de su época y el mayor de la historia de la India.

Srinivasa Ramanujan

Ramanujan nació el 22 de diciembre de 1887 en Erode, una pequeña población situada a unos 400 km de Madrás, en el seno de una familia humilde. A los siete años consiguió una beca que le permitió asistir a clases en un colegio de Kumbakonam. Sus extraordinarias cualidades numéricas, tanto memorísticas como

de cálculo, se manifestaron ya desde su más tierna infancia. Era capaz de repetir de memoria cientos de decimales del número *n* o de la raíz cuadrada de dos. El primer texto de matemáticas que cayó en sus manos fue *Synopsis of Elementary Results in Puré Mathematics*, de G. S. Carr. Tenía entonces 15 años y puede considerarse que con él llevó a cabo su primera labor investigadora, ya que se trataba de un texto sintético, en el que apenas había demostraciones y que, dada la situación de precariedad matemática en la que se encontraba, tenía que resultarle prácticamente incomprensible.



Sello indio emitido en 1962 en conmemoración del 75º aniversario del nacimiento de Srinivasa Ramanujan.

A los 16 años consiguió una beca para ingresar en el College del Gobierno de Kumbakonam. Pero la pasión que Ramanujan sentía por las matemáticas lo llevaba a emplear todo su tiempo en ellas y, por consiguiente, dejó abandonadas las demás asignaturas, por lo cual acabó perdiendo la beca. A partir de entonces nunca aprobó ninguna asignatura que no fuera de matemáticas.

En 1909 se casó y se vio obligado a buscar un trabajo que le permitiera mantener a su familia. A través de un amigo consiguió una carta de recomendación para colaborar con un aficionado a las matemáticas, Diwan Behadur R. Ramachandra

Rao, que era recaudador de Nelore, a 130 km al norte de Madrás. La primera entrevista con Ramanujan la describe de este modo:

«Hace algunos años, un sobrino mío, ignorante por completo de todo conocimiento matemático, me dijo: “Tío, tengo un visitante que habla de matemáticas y no lo comprendo. ¿Podría mirar si hay algo de interés en su charla?”. Y en la plenitud de mi sabiduría matemática, condescendí a que Ramanujan se acercara a mi presencia. Una pequeña figura rústica, vigorosa, sin afeitar, desaliñada, con un rasgo llamativo, ojos brillantes, entró con un gastado libro de notas bajo el brazo. Era extremadamente pobre.

Había huido de Kumbakonam a Madrás con el fin de conseguir cierto desarrollo para proseguir sus estudios. Jamás pidió ninguna distinción. Necesitaba desahogo. En otras palabras, que le suministrara el mínimo vital sin esfuerzo de su parte y que se le permitiera soñar. Abrió el libro y comenzó a explicar algunos de sus descubrimientos. Al punto vi claramente que era algo fuera de lo corriente, pero mis conocimientos no permitieron juzgar si hablaba con sentido o sin él. Suspendido todo juicio le pedí que viniera de nuevo y así lo hizo. Apreció debidamente mi ignorancia y me demostró algunos de sus hallazgos más simples. Éstos iban más allá de los libros existentes y ya no tuve duda de que era un hombre notable. Después, paso a paso, me inició en las integrales elípticas y en las series hipergeométricas y, finalmente, su teoría de las series divergentes, no divulgada todavía, me convenció. Le pregunté qué era lo que deseaba. Dijo que quería una pequeña pensión para vivir y así proseguir sus investigaciones».

Ramanujan, que no aceptaba vivir de ningún tipo de caridad, aceptó finalmente un trabajo como contable en la Compañía del Puerto de Madrás. A pesar de que, como persona responsable que era, daba cumplimiento a sus obligaciones en la compañía, su mente y su alma sólo albergaban un objetivo: tener los medios suficientes para cubrir sus necesidades y las de su familia y poder dedicarse a las matemáticas.

Ramanujan poseía también el «don de los números» al que hemos hecho referencia en capítulos anteriores. Hay un par de anécdotas que dan fe de este don. La primera de ellas la relata P. C. Mahalanobis (1893-1972), uno de sus colegas indios en Cambridge, que se estaba entreteniendo en resolver un problema de lógica matemática que aparecía en un diario. Después de varios minutos de hacer pruebas

encontró la solución adecuada, que consistía en un par de números. Le propuso entonces a Ramanujan, que en aquel momento se estaba preparando la comida (era vegetariano estricto): «Aquí hay un problema para ti...», y se lo leyó. Ramanujan, al instante, y sin dejar de trajinar con las sartenes, le contestó: «Apunta la solución...». Y le dio una fórmula general para obtener infinitos pares de números, todos los cuales eran solución al problema. El primer término era la solución que Mahalanobis había encontrado.

La segunda sucedió en el verano de 1917. Ramanujan había ingresado con síntomas de tuberculosis en Putney, un sanatorio de Cambridge. Su amigo y mentor, el matemático británico Hardy, fue una mañana a visitarlo. «Recuerdo que fui a verlo cuando yacía enfermo en Putney», relata el mismo Hardy.

> *«Yo había viajado en el taxi número 1.729 y observé que el número me parecía más bien insípido y esperaba que no le fuera de mal agüero. "No —contestó— es un número muy interesante. Es el número más pequeño expresable como suma de dos cubos de dos maneras diferentes"».*



Casa de Ramanujan en Kumbakonam, ciudad en la que el matemático indio falleció el 26 de abril de 1920.

En efecto,

$$1.729 = 1^3 + 12^3 = 9^3 + 10^3.$$

«Le pregunté, naturalmente, si conocía la respuesta al problema correspondiente para la cuarta potencia y él replicó, después de un momento de reflexión, que el ejemplo no era obvio y que el primero de tales números debía de ser muy grande».

Ramanujan se había dejado tentar por la rama de las matemáticas que Hardy consideraba más difícil, la teoría de números. Y muy pronto cayó en la «trampa» que, desde hacía dos mil años, los números primos habían tendido a todos los matemáticos que se habían aventurado por sus oscuros senderos. Ramanujan se había propuesto encontrar la «fórmula mágica», aquella mediante la cual se pudieran descubrir todos los números primos. Este empeño le llevaría, inevitablemente, a enfrentarse con problemas de envergadura, como el estudio de las series divergentes.

Pero llegó un punto en que su situación económica y social no le permitía seguir avanzando. Los matemáticos de los que estaba rodeado no podían ayudarle. Entre varios amigos redactaron una carta en inglés que hicieron llegar a varios matemáticos europeos en la que Ramanujan manifestaba sus conocimientos y el deseo de poder ampliarlos. La carta decía así:

Apreciado señor:

Me permito presentarme a usted como un oficinista del departamento de cuentas del Port Trust Office de Madrás con un salario de 20 libras anuales solamente. Tengo cerca de 23 años de edad. No he recibido educación universitaria, pero he seguido los cursos de la escuela ordinaria. Una vez dejada la escuela he empleado el tiempo Ubre de que disponía trabajando en matemáticas. No he pasado por el proceso regular convencional que se sigue en un curso universitario, pero estoy siguiendo una trayectoria propia. He hecho un estudio detallado de las series

divergentes en general y los resultados a que he llegado son calificados como «sorprendentes» por los matemáticos locales...

Yo querría pedirle que repasara los trabajos aquí incluidos. Si usted se convence de que hay alguna cosa de valor me gustaría publicar mis teoremas, ya que soy pobre. No he presentado los cálculos reales ni las expresiones que he adoptado, pero he indicado el proceso que sigo. Debido a mi poca experiencia tendría en gran estima cualquier consejo que usted me diera. Pido que me excuse por las molestias que ocasiono.

Quedo, apreciado señor, a su entera disposición,

S. Ramanujan.

De todos aquellos matemáticos que recibieron la carta de Ramanujan, sólo Hardy supo percatarse del valor de aquellos escritos. Ramanujan le había enviado cerca de 120 teoremas que contenían multitud de fórmulas. Refiriéndose a ellas, Hardy comentó: «Nunca había visto antes nada, ni siquiera parecido a ellas. Una hojeada es suficiente para comprender que solamente podían ser escritas por un matemático de la más alta categoría. Tenían que ser ciertas, porque, si no lo hubiesen sido, nadie habría tenido suficiente imaginación para inventarlas».

Godfrey Harold Hardy (1877-1947)

Hardy fue un personaje pintoresco, con un sentido del humor típicamente británico y un círculo de amistades muy restringido. Un día decidió establecer una valoración personal sobre los matemáticos: puntuaba su talento en una escala de 0 a 100. No tuvo reparos en hacerla pública, y en dicha valoración se dio a sí mismo una puntuación de 25, mientras que otorgó un 30 a Littlewood y un 80 a Hilbert (por cierto, era su mejor amigo y el matemático con el que más colaboraciones tuvo). A Ramanujan le concedió la máxima puntuación.



Según declaró el propio Hardy, su mayor contribución a las matemáticas fue el descubrimiento de Ramanujan.

En mayo de 1913, Hardy le consiguió una beca para que se trasladara a Cambridge, pero Ramanujan renunció porque su madre no le autorizó a trasladarse a Inglaterra. Al cabo de poco tiempo le dio permiso. Las razones, según relata Hardy, fueron que «una mañana, su madre declaró que la noche anterior había visto a su hijo, en una gran sala, rodeado de un grupo de europeos y que la diosa Namagiri le había ordenado que no se interpusiera en el camino de su hijo y que colaborara al objeto de su vida».

Por fin, y gracias a los esfuerzos de Hardy, Ramanujan pudo trasladarse a Cambridge con una beca procedente en parte de Madrás y en parte del Trinity College. A partir de ese momento la tarea del matemático inglés, que sería su maestro, fue tan ardua como difícil. ¿Qué método debía seguirse para enseñarle matemáticas modernas? «Las limitaciones de su conocimiento eran tan asombrosas como su profundidad», se lamentaba Hardy. La dificultad crecía dada la enorme variedad de temas que Ramanujan había abordado, en los que se mezclaban resultados nuevos con otros que ya habían sido demostrados. En gran medida,

Ramanujan debía ser reeducado, pero Hardy intentó siempre no romper, con excesivos formalismos, lo que él llamaba el «encanto de su inspiración».

Ramanujan vivió cinco años en Cambridge, tiempo durante el cual publicó veintiún artículos, cinco de ellos en colaboración con Hardy, quien acabó manifestando: «Yo aprendí de él mucho más de lo que él aprendió de mí».

En la primavera de 1917 aparecieron los primeros síntomas de la tuberculosis que acabaría con la vida de Ramanujan. Aquel mismo verano ingresó en el sanatorio de Cambridge. El resto de su vida lo pasaría más tiempo en la cama que fuera de ella. En otoño de 1918, y coincidiendo con una cierta mejoría de su salud, llegó la tan esperada elección para una Trinity Fellowship, lo que le levantó el ánimo para reemprender de nuevo su trabajo, haciendo de ésta una de sus épocas más productivas. A comienzos de 1919 volvió a la India, donde murió al año siguiente.

Números Taxicab

Desde aquel encuentro en la clínica entre Ramanujan y Hardy, a los números que tienen la propiedad de ser los más pequeños que se pueden expresar como suma de n cubos de dos maneras diferentes se les llama taxicab y se definen así: «El número taxicab n-ésimo es el número natural más pequeño que se puede expresar de n formas distintas como suma de dos cubos positivos». Actualmente los números taxicab conocidos son:

Ta (1) = 2;

Ta (2)= 1.729;

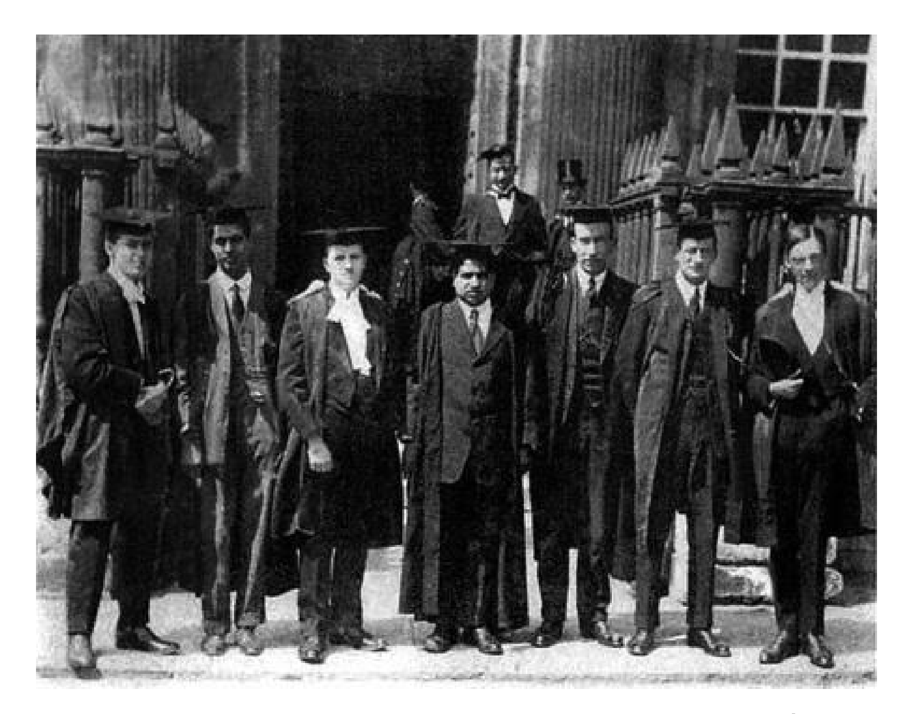
Ta (3) = 87.539.319;

Ta (4) = 6.963.472.309.248;

Ta (5) = 48.988.659.276.962.496.

El sexto taxicab, Ta (6), todavía no se conoce.

La mayor parte de su obra se encuentra en forma epistolar y también recogida en tres cuadernos personales, uno de ellos perdido y reencontrado en 1976. La revisión total de su trabajo todavía no ha concluido, ya que, a pesar de haber fallecido a los 33 años, legó más de 4.000 teoremas al universo de las matemáticas.



Ramanujan (en el centro) y Hardy (derecha), en una fotografía de grupo a las puertas del Trinity College de Cambridge.

Los trabajos de Ramanujan sobre los números primos, concretamente el hallazgo de una fórmula exacta para su obtención, están rodeados de cierto halo de misterio, aunque en cierto modo se pueden considerar un fracaso. Hardy comentó al respecto:

> *«A pesar de que Ramanujan tuvo numerosos y brillantes éxitos, sus trabajos sobre los números primos y sobre todos los problemas relacionados con esta teoría estaban ciertamente equivocados. Puede decirse que éste fue su único gran fracaso. Pero todavía no estoy convencido de que, de alguna manera, su fracaso no fuera más maravilloso que cualquiera de sus triunfos...».*

Vida ordenada

Ramanujan seguía una escrupulosa vida de Brahmín, la casta hindú de más elevada espiritualidad, con un estricto autocontrol y una frugalidad ascética, que excluía de su dieta todos los productos animales e incluso muchos vegetales, como el ajo y la cebolla. Es curioso reparar en que,

durante toda su vida, era al levantarse de la cama cuando escribía precipitadamente sus hallazgos, de muchos de los cuales no era capaz de encontrar una demostración rigurosa.

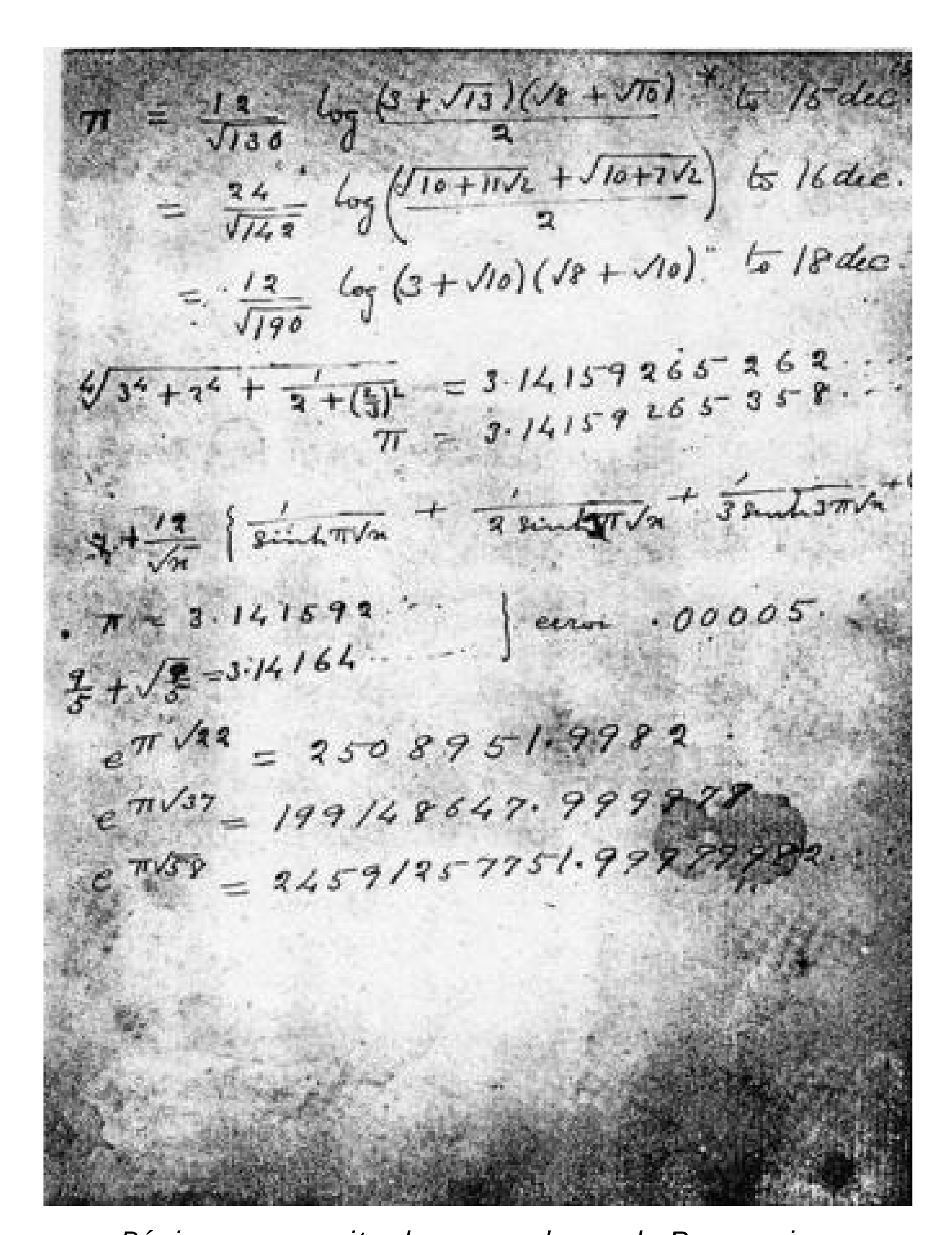
Ramanujan no conocía la obra de Riemann ni la de Gauss, pero estaba dispuesto a encontrar una fórmula que le proporcionase la lista de los números primos. Decía poseer una para saber con absoluta precisión la cantidad de números primos menores que un número dado cualquiera. Entre los resultados que envió a Hardy no había demostraciones de ninguna de sus afirmaciones. Había, en cambio, una fórmula que estuvo a punto de dar al traste con las ambiciones de Ramanujan:

$$1 + 2 + 3 + 4 + \ldots + \infty = {}^{1}/_{-12}$$

Lo absurdo de esta igualdad hacía pensar que el autor no era más que un charlatán sin apenas conocimiento de lo que podía ser una serie convergente. Pero la perspicacia matemática de Hardy intuyó, por el resto de los resultados matemáticos que acompañaban al paquete, que allí debía de haber gato encerrado. El error de interpretación se resolvió cuando se dieron cuenta de que había una confusión en el sistema de notación y que lo que Ramanujan había puesto en sus manos era ni más ni menos que uno de los ceros de la función zeta de Riemann, concretamente la solución para $x = -1$. El método que Ramanujan decía poseer le proporcionaba una fórmula para obtener el número de primos que había entre uno y cien millones con un asombrosamente bajo margen de error. Littlewood demostró que Ramanujan estaba equivocado. La búsqueda de la fórmula mágica lo llevó, como a tantos otros matemáticos, a adentrarse en parajes sumamente fructíferos y que, como también en otros muchos casos, tenían una relación directa con las series convergentes.

El matemático americano Bruce Berndt, profesor del departamento de matemáticas de la Universidad de Illinois, que ha dedicado gran parte de su tiempo al estudio de las obras de Ramanujan, descubrió que éste había elaborado una tabla, diferente de la primera que había hecho llegar a Hardy, en la que se estudia con mayor detalle y precisión la aparición de números primos entre los cien primeros millones de números naturales. Berndt afirma que la precisión es aún mayor que la conseguida

mediante la fórmula de Riemann, lo que le lleva a especular con la posibilidad de que Ramanujan poseyera realmente una fórmula que, por algún motivo, no diera a conocer a nadie. Es muy probable que entre los cuadernos personales de Ramanujan queden todavía muchas verdades por desvelar.



Página manuscrita de un cuaderno de Ramanujan

Es cierto que la exótica mente matemática de Ramanujan produjo algunos resultados aparentemente falsos, pero en su mayor parte dio resultados ciertos y de

una gran belleza matemática. En cualquier caso, sus trabajos ocupan actualmente a miles de matemáticos en los departamentos de las universidades, y sus resultados se aplican en áreas tan dispares como la química de los polímeros, la arquitectura de los ordenadores o la investigación del cáncer.

Capítulo 7
¿Para qué sirven los números primos?

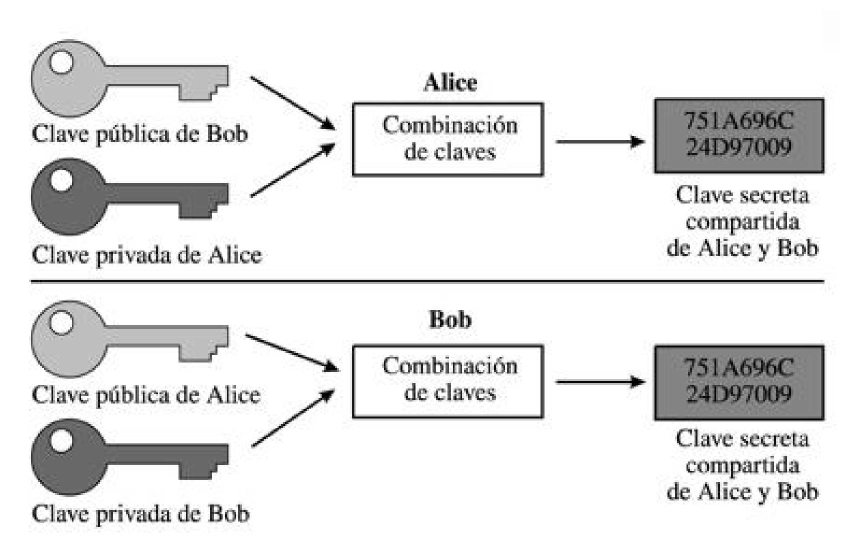
Contenido:

1. *Los números primos en la criptografía*
2. *Los tiempos del ordenador*
3. *P versus NP*
4. *Fabricar números primos*
5. *¿Cómo saber si un número es primo?*
6. *Pseudoprimos*
7. *Los métodos*
8. *Y la historia continúa...*

Encontrar números primos, se entiende que números primos grandes, no es una tarea sencilla, porque, como ya hemos visto, todavía nadie ha sido capaz de encontrar la fórmula, el algoritmo que nos permita construir números primos a discreción. Ante esta situación, algunas personas se pueden plantear la siguiente pregunta: «¿Para qué queremos construir números primos?». Hay dos respuestas. La primera es que tiene un interés teórico. El intento promueve el nacimiento de herramientas de cálculo interesantes, especialmente de cálculo informático. Además, disponer de descomunales listas de números primos sirve también para comprobar teoremas que aún no han sido demostrados. Si alguien lanza una conjetura sobre números primos y se puede comprobar que hay uno, aunque sea de millones de cifras, que no la cumple, la cuestión queda zanjada. Esto ha desencadenado una búsqueda de números primos de todas familias, de Mersenne, gemelos, etc., que en algunos casos ha llegado a tener un carácter que podríamos calificar de competitivo, inscrito en el mundo de los récords y de los grandes premios. Pero también hay otra razón, de índole práctica, que guarda estrecha relación con las llamadas claves criptográficas: el correo electrónico, las transacciones bancarias, las tarjetas de crédito o las comunicaciones por teléfono móvil se protegen mediante claves secretas que se basan directamente en las propiedades de los números primos.

1. Los números primos en la criptografía

En 1975, W. Diffie y M. Hellman, de la Universidad de Stanford, desarrollaron la idea de los cifrados asimétricos o de «clave pública», un sistema basado en determinadas funciones matemáticas, llamadas «de una sola dirección» o «funciones con trampa», que hacen posible el cifrado, pero virtualmente imposible el descifrado si no se conoce la clave. La idea es que cada usuario posea un par de claves, una pública y otra privada. Si quiero enviar un mensaje a una persona, cifro el mensaje según su clave, que es pública, en el sentido de que cualquiera puede conocerla, pero sólo ella, con su clave privada, la puede descifrar. Una de las ventajas de este método es que la clave privada nunca circula por los medios de comunicación y, por tanto, no es necesario renovarla constantemente.



Esquema del principio teórico que subyace a los cifrados del tipo Diffie-Hellman. Supongamos dos emisores/receptores, Atice y Bob. Ambos acuerdan públicamente dos parámetros (un número primo p y otro número g, con ciertas propiedades). Tanto Alice como Bob operan sobre dichos parámetros mediante un número entero, que mantienen privado, y se envían públicamente el resultado de dicha operación. Alice y Bob operan esta segunda expresión y llegan a un mismo valor, que ahora puede servir como clave secreta compartida. Un potencial espía que haya interceptado las comunicaciones públicas de Alice y Bob no podrá, a partir de esta información, generar la clave secreta.

No se trata de un tema sencillo, pero podemos intentar comprenderlo mediante una analogía. Imaginemos un gran almacén de pinturas en el que disponemos de cientos de miles de botes de distintos colores.

Tomamos dos botes cualesquiera y hacemos una mezcla con diferentes cantidades de pintura de cada bote. Hasta aquí, se trata de una operación sencilla. Pero si ahora le mostramos el resultado a alguien y le pedimos que «descifre» las cantidades de colores que han intervenido en la mezcla final lo ponemos ante un problema de difícil solución.

Éste es el mecanismo de las funciones matemáticas con trampa o de una sola dirección, en las que es muy fácil «ir» pero prácticamente imposible «volver». Supongamos ahora que en el almacén, en vez de botes de pintura tenemos números primos. Tomamos dos al azar, por ejemplo el 7 y el 13, y los multiplicamos, operación análoga a mezclar los botes de pintura, con el resultado de 7 x 13 = 91.

La pregunta que se plantea entonces es la siguiente: «¿Se puede saber qué dos números primos multiplicados entre sí dan 91 como resultado?». Es cuestión de tener una lista de números primos e ir haciendo pruebas. La cosa parece sencilla, como lo sería también la de averiguar los colores que forman la mezcla de pinturas si en el almacén no hubiera más que una docena de colores básicos. Pero las cosas no son así y mucho menos con los números primos.

Averiguar, por ejemplo, que el número 1.409.305.684.859 es el resultado de multiplicar los dos números primos 705.967 y 1.996.277 puede poner a prueba la paciencia de cualquiera, sobre todo si se tiene en cuenta que estos dos números primos se han extraído de una lista en la que figuran todos aquellos que hay entre el número 1 y el número 2.000.000, que son la friolera de 148.933.

Pero, como hemos venido insistiendo hasta ahora, vivimos en la era de la informática y éste es un asunto que, en un principio, un buen programa implementado en un potente ordenador puede resolver en poco tiempo... hasta cierto punto, ya que todo depende de lo grande que sea el almacén de pinturas, y hay que insistir en que el de los números primos no sólo es muy grande, sino que es infinito.

El par de números primos del anterior ejemplo tenía pocas cifras. Si se toman primos con cientos de cifras cada uno, el tiempo de espera de ese programa de ordenador, que al fin y al cabo está buscando los números «a lo bestia» o, como se dice en la jerga criptográfica, mediante un ataque de «fuerza bruta», puede llegar a superar con mucho el tiempo de vida en la Tierra.

El RSA 129

Es famoso el «derribo» del RSA 129, que se produjo en abril de 1994. Se trataba de un número de 129 cifras que los autores del sistema habían hecho público, planteándolo como reto. Un grupo de 600 matemáticos, con la ayuda de 1.600 voluntarios reclutados en Internet, consiguieron factorizar el número. Sin embargo, se calcula que poniendo a trabajar todos los ordenadores del mundo en paralelo, una clave de 1.024 dígitos tardaría un tiempo equivalente a la edad del universo (13.700 millones de años) en romperse. Piénsese que en la criptografía de clave pública se utilizan números de 128, 1.024 y hasta 2.048 bits. Cuantas más cifras tenga el sistema, más robusto será frente a un ataque, pero también tiene el inconveniente de que el proceso de desencriptado es más lento.

Si es cierto que los números primos están totalmente inmersos en nuestra vida cotidiana, como la tarjeta de crédito o el ordenador personal, debe existir forzosamente una demanda de números primos, ya que para construir una clave secreta hacen falta un par de ellos. Existe un «mercado» de números primos que mantiene una producción a gran escala de grandes números primos, pero en estos menesteres es tan importante la producción como el control de calidad. Para que un número muy grande adquiera la categoría de primo debe ser testado por algún organismo reconocido oficialmente.

El sistema RSA se publicó en 1978, pero su uso generalizado como clave criptográfica no tuvo lugar hasta finales de la década de 1990, con la implantación de Internet. La obtención de números primos grandes era difícil, ya que requería de un software muy concreto, y lo que se hacía era comprarlos a empresas especializadas o a ciertos departamentos universitarios que los obtenía como

resultado de sus propias investigaciones. Pero el crecimiento exponencial de la capacidad de cálculo de los ordenadores junto con la constante aparición de algoritmos de implementación más sofisticados ha ido transformando el mercado de los números primos: en poco tiempo su adquisición se ha hecho mucho más asequible.

2. Los tiempos del ordenador

La aparición de los logaritmos supuso un importante ahorro de tiempo y energía que hasta entonces se empleaba en engorrosos cálculos carentes de valor matemático. Más tarde aparecieron la regla de cálculo y las primeras máquinas calculadoras mecánicas, en las que había que hacer girar una serie de rodillos para obtener los resultados de sumas y productos.

Pero fueron los ordenadores los primeros que empezaron a hacer cálculos que iban mucho más allá de la capacidad de la mente humana. Y llegó el momento en que las máquinas fueron capaces de llevar a cabo la simulación de un razonamiento deductivo, algo propio de una mente matemática. En aquel momento algunos científicos tuvieron la sensación de que se estaba traspasando una frontera a la que, hasta entonces, no había tenido acceso ningún tipo de máquina.

¿Era buen juicio o prejuicio? El desarrollo de la informática, con su crecimiento exponencial, estaba empezando a cambiar paradigmas forjados durante siglos. Aparecieron los primeros algoritmos computacionales capaces de demostrar teoremas.

Los detractores de las demostraciones con ordenador aducen básicamente dos razones para poner en tela de juicio este procedimiento. La primera es que no son verificables, ya que contienen etapas en el programa que nunca podrán ser comprobadas por ningún matemático. La segunda es que el proceso está sometido a errores, tanto de software como de hardware. En la mayoría de los casos se trata de errores aleatorios. Una manera de paliar estos defectos consiste en implementar diferentes programas en otras máquinas para ver si conducen al mismo resultado.

Esto supone una cierta limitación, ya que cuando se trata de números que no están expresados en base 2, tienen que hacer aproximaciones, lo cual los deja sometidos a posibles errores.

En 1991, David R. Stoutemyer llevó a cabo 18 experimentos de cálculo con programas de ordenador que dieron resultados incorrectos.



Se calcula que el superordenador Cray comete un solo error cada mil horas de funcionamiento.

Esto ha llevado a que muchos consideren que esta nueva forma de hacer matemáticas es más propia de las ciencias empíricas o experimentales. Pero nadie ha decidido que el quehacer matemático haya sido concebido para siempre de una sola forma. Tampoco el razonamiento matemático «tradicional» ha estado exento de errores a lo largo de su historia. Más de un resultado falso se ha estado dando por bueno durante años. Además, en nuestros días las matemáticas han alcanzado un nivel de diversidad y de complejidad tan alto que la verificación de un teorema puede llevar años o, en el mejor de los casos, quedar en manos de unos cuantos especialistas. En definitiva, son muchos los expertos que actualmente opinan que la utilización del ordenador como herramienta de investigación e incluso de verificación de teoremas ha dado nacimiento a una manera diferente de concebir las matemáticas. No sería descabellado imaginar que algún día se acepte una demostración de la conjetura de Riemann realizada por un ordenador.

Máxima seguridad

El gobierno de Estados Unidos sólo permite la utilización de determinadas claves criptográficas en su territorio y en Canadá; fuera de estas fronteras no se autoriza la venta, a no ser que se trate de una entidad financiera. La exportación no autorizada de estándares de encriptación está considerada como tráfico de armas. Las empresas que se dedican a la fabricación de programas de encriptación almacenan las claves secretas en una especie de «pastillas» dotadas de sofisticados dispositivos de seguridad. Cuando se abren, al entrar en contacto con el oxígeno, se solidifican en una masa informe; si se intenta verlas con rayos X, todo lo que hay escrito en ellas se convierte en ceros.

En cualquier caso, nadie puede poner en duda la validez de los métodos computacionales para encontrar números primos e incluso para verificar si un número lo es. Cuando nos adentramos en el mundo del álgebra computacional empiezan a aparecer términos como «polinomial», «polinomial determinista», o «probabilístico», que se manejan con absoluta soltura, pero que dejan completamente fuera de juego a los legos en la materia. Aunque sea a modo de apunte, es aconsejable tener una idea aproximada de los conceptos que encierran estos términos.

Cuando se habla de tiempo polinomial (o polinómico) se hace referencia al tiempo que tarda la máquina en resolver un cierto algoritmo. Supongamos que tenemos una variable de entrada a la que podemos llamar n. En general, cuando el algoritmo utilice una expresión de tipo polinomial, como $n^3 + 2n + 1$, diremos que se trata de un algoritmo en tiempo polinomial (P), mientras que si se utilizan expresiones de tipo exponencial, como 5^n, estaríamos hablando de un algoritmo no polinomial. La idea básica es, en términos muy generales, que los algoritmos polinomiales tienen un tiempo de ejecución razonable, mientras que los exponenciales, no.

3. P versus NP

Ya hemos visto que en computación se crea una serie de problemas que se pueden resolver de una forma determinista, es decir, con una solución en la que existen

garantías de validez; para ello se utilizan algoritmos de tipo polinomial que se desarrollan en tiempo polinomial. El ejemplo más sencillo sería el de hacer sumas, productos o la resolución de un gran número de ecuaciones. En la mayoría de los casos, mediante algoritmos adecuados, el tiempo de resolución se puede mantener dentro de intervalos aceptables.

A todos los problemas que pueden ser tratados de esta forma se los considera problemas de tipo P.

Por el contrario, se denominan problemas NP a aquéllos para los que se puede encontrar un tipo de solución indeterminista, a base de probar soluciones que tal vez sean ciertas. Los tiempos de resolución para este tipo de problemas son muchísimo más rápidos que los empleados para los problemas de tipo P. Está claro que cualquier problema que admita una solución determinista en tiempo polinomial es también un problema al que se le puede aplicar una solución para una comprobación de tipo rápido. Dicho en otras palabras, todo problema de tipo P es de tipo NP.

Pero, llegados a este punto, es preciso aclarar el concepto de algoritmo.

Un algoritmo viene a ser como una receta de cocina, es decir, está constituido por una serie de instrucciones que no deben dejar lugar a dudas. Por ejemplo, para resolver una ecuación como $x - 2 = 8$, el algoritmo de resolución diría algo así como:

1. Despejar x (pasar al otro miembro de la ecuación cualquier otro número cambiándole el signo): $x = 8 + 2$.
2. Hacer la operación correspondiente en el segundo miembro: $8 + 2 = 10$.
3. Escribir la solución: $x = 10$.

Éste sería un problema de tipo P que llevaría su correspondiente tiempo polinomial de resolución, si bien este ejemplo es un caso trivial muy rápido de solucionar.

Se entiende que podríamos probar soluciones como $x = 3$; $x = -2$, etc., y que el tiempo de computación sería mucho más rápido, ya que lo único que tiene que hacer el programa es colocar un valor en lugar de la x y comprobar si la solución es cierta. No es determinista en el sentido de que habrá cierta probabilidad de que la solución sea errónea (se entiende que disponemos de algún criterio que permita

acotar el rango de soluciones, como, por ejemplo, saber que tienen que estar todas comprendidas entre 9 y 11).

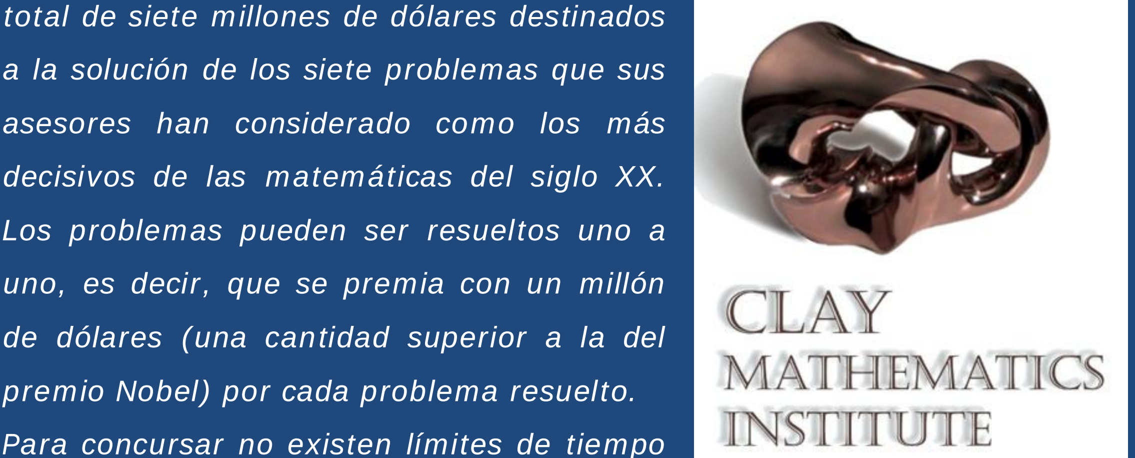
La pregunta inversa consiste en lo siguiente. Si yo tengo un algoritmo de comprobación ¿puedo garantizar que existe un algoritmo polinomial que me permita resolver de manera determinista el problema (que es casi tanto como preguntarse si podemos estar seguros de que existirá algún tipo de algoritmo para buscar la solución en tiempo polinomial)?

Los siete problemas del milenio

El Clay Mathematics Institute (CMI) es una fundación privada sin fines lucrativos que fue creada por Landon T. Clay, un empresario multimillonario de Boston.

Su objetivo es el desarrollo y la divulgación del conocimiento matemático.

El 25 de mayo de 2000, el instituto anunció la creación de los «Millennium Prize Problems», premio financiado con un total de siete millones de dólares destinados a la solución de los siete problemas que sus asesores han considerado como los más decisivos de las matemáticas del siglo XX. Los problemas pueden ser resueltos uno a uno, es decir, que se premia con un millón de dólares (una cantidad superior a la del premio Nobel) por cada problema resuelto.



Para concursar no existen límites de tiempo ni de edad, ni son necesarios currículos universitarios. Los siete problemas seleccionados son:

1. *El problema P versus NP.*
2. *La conjetura de Riemann.*
3. *La teoría de Yang-Mills.*
4. *Las ecuaciones de Navier-Stokes.*
5. *La conjetura de Birch y Swinnerton-Dyer.*
6. *La conjetura de Hodge.*

7. La conjetura de Poincaré.

Dada la dificultad y trascendencia de los problemas propuestos, los asesores financieros del Sr. Clay tenían serias dudas de que el Instituto tuviera que deshacerse alguna vez del dinero de los premios. Sin embargo, en 2006, el ruso Grigori Perelman sorprendió a propios y extraños con la solución del séptimo y último problema, la conjetura de Poincaré. No obstante, rechazó, por motivos personales, la Medalla Fields que le fue otorgada en el marco del XXV Congreso Internacional de Matemáticos celebrado en Madrid.

Éste fue el problema que de manera independiente se plantearon en 1971 Stephen Cook y Leonid Levin: Si todo problema P es NP, ¿existen problemas NP que no sean P? Éste se considera el mayor reto que tiene planteada la computación actual y forma parte de uno de los Problemas del Milenio según los establece el Instituto Clay, de manera que quien lo resuelva tiene la garantía de que dicha institución lo recompensará con la nada despreciable cifra de un millón de dólares.

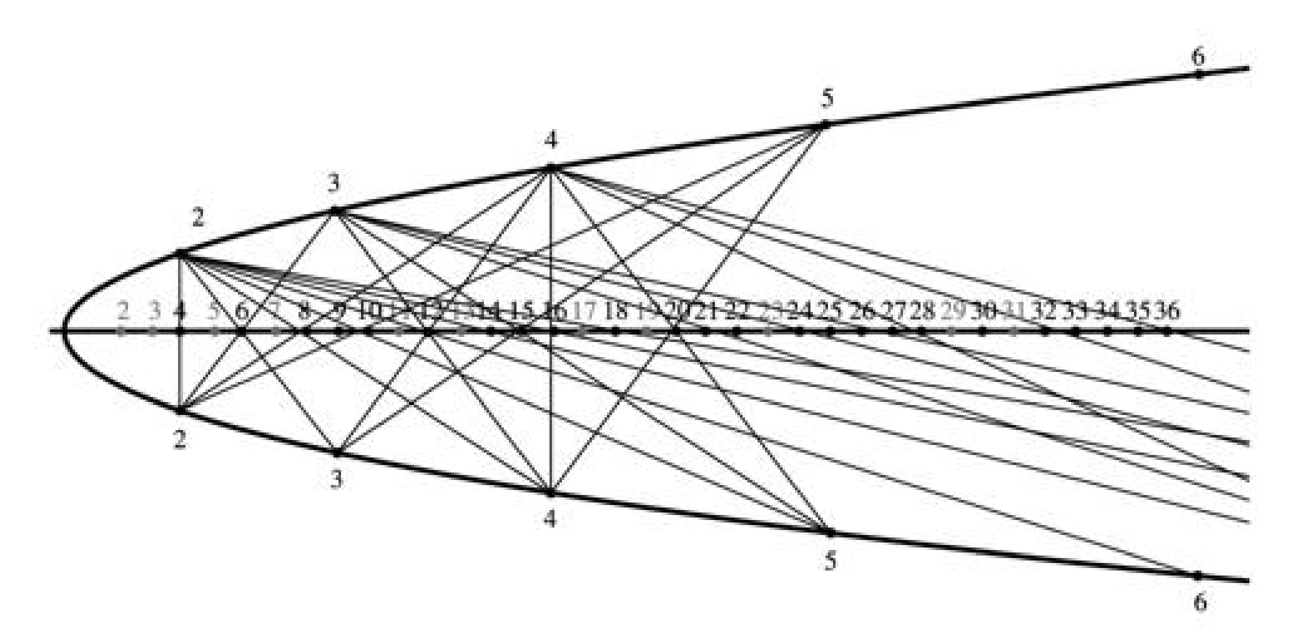
4. Fabricar números primos

Es frecuente que alguien sin demasiada cultura matemática haga gala de haber encontrado, casi siempre en Internet, un sistema o fórmula para averiguar cuál es el siguiente número primo para un número natural *n*. Sólo hay que pensar que una noticia de este calibre no debería tener que buscarse, pues dadas sus repercusiones, si alguien hubiera encontrado la fórmula mágica y la hubiera dado a conocer habría saltado a las primeras páginas de los periódicos y noticiarios de todo el mundo.

Existen muchos modelos geométricos para encontrar números primos. A veces, éstos pueden llevar a engaño a los incautos, ya que se presentan como fórmulas que permiten hallar todos los números primos, cuando en realidad no son más que variantes de la criba de Eratóstenes o diferentes formas de llevar a cabo la criba mediante métodos geométricos. Y la verdad es que hay algunos realmente ingeniosos.

Uno de los más interesantes es el que crearon los matemáticos rusos Yuri Matiyasevich (n. 1947) y Boris Stechkin (1920-1995) valiéndose de una parábola. Ésta se representa con sus dos ramas y en el eje de la misma se escribe la sucesión de los números naturales. Luego se levanta una perpendicular que se corresponda con el cuadrado de cada número, es decir, que en el lugar en que está el 4 se levanta la perpendicular que se corresponde, en cada una de las dos ramas, con el número 2. El significado geométrico de la perpendicular es que se ha realizado el producto de 2 por sí mismo. Del mismo modo, tendríamos otra perpendicular para simbolizar el producto de 3 por sí mismo y la levantaríamos en el punto 9 del eje. Y así sucesivamente.

Cuando ya se tienen todos estos números representados por puntos en la parábola, se une cada punto de una rama con todos los de la otra. O sea, el punto 2 de la rama superior lo unimos con el 2, 3, 4, 5,… de la inferior. Cada uno de estos segmentos corta al eje en el producto correspondiente. Si se llevan a cabo todas las intersecciones posibles, los únicos puntos de la parábola por los que no pasa ningún segmento son precisamente los números primos. Éste es un ejemplo de una criba de tipo geométrico.



Criba geométrica de Yuri Matiyasevich y Boris Stechkin para la búsqueda de números primos, que aparecen de color gris en la ilustración. Obsérvese que por ellos no pasa ningún segmento.

Las cribas de tipo algebraico están más encaminadas a obtener algoritmos computacionales rápidos. Una de ellas es la criba de Atkin, ideada por A. O. L. Atkin y Daniel J. Bernstein, que permite hallar todos los números primos menores o iguales que un número natural dado. En ciertos aspectos es una versión mejorada de la criba de Eratóstenes. Cuando decimos mejorada nos estamos refiriendo más bien a actualizada, ya que la criba de Atkin, aritméticamente hablando, presenta algunas deficiencias con respecto a la de Eratóstenes, puesto que requiere de una preparación previa y no elimina los múltiplos de los números primos, sino sólo los múltiplos de los cuadrados de los primos.

Ya sabemos que lo ideal sería poder encontrar una fórmula que asociara a cada número natural *n* el *n*-ésimo número primo. Hemos visto que los matemáticos llevan más de tres mil años buscando dicha fórmula. Lo que sí existen son funciones que permiten calcular de forma práctica números primos. Por ejemplo, se demuestra (teorema de Wilson) que *p* es un número primo si y sólo si $(p - 1)! \equiv -1 \ (mod\ p)$, pero, como ya explicamos anteriormente, cualquier fórmula que incluya factoriales es inviable a la hora de implementar un algoritmo en una computadora, debido al rápido crecimiento de la función que hace demasiado largos los tiempos de computación.

Existen también polinomios que «fabrican» números primos, como el que utilizó Euler para calcular una lista de cuarenta números primos mediante la función $f(x) = x^2 + x + 41$, que proporciona números primos dando valores a X. Por ejemplo,

$$x = 0 \quad f(0) = 0 + 0 + 41 = 41$$

$$x = 1 \quad f(1) = 1 + 1 + 41 = 43$$

$$x = 2 \quad f(2) = 4 + 2 + 41 = 47$$

Sin embargo, la fórmula empieza a fallar para valores de *x* mayores que 41. Por ejemplo, para ese mismo valor, x = 41, la expresión da como resultado un número compuesto:

$$x = 41\ f(41) = 1.681 + 41 + 41 = 1.763.$$

Euler prosiguió investigando en dicho polinomio y llegó a la conclusión de que un polinomio más general, como $x^2 - x + q$, podría proporcionar números primos para valores de x comprendidos entre 0 y $q - 2$. Existen también polinomios, como el descubierto por Jones, Sato, Wada y Wiens en 1976, que proporcionan sólo números primos cuando se da valores a sus variables. Se trata de un polinomio de veintiocho variables y de complejidad un tanto desproporcionada. No tiene un excesivo interés práctico: cuando el valor producido es positivo, se trata siempre de un número primo, pero la mayoría de las veces, por no decir casi todas, el resultado es un número negativo.

Actualmente, la mayor parte de los números primos conocidos (en este contexto hablamos siempre de números primos grandes) son los llamados primos de Mersenne. Esto es debido a que existe un test de primalidad, el test de Lucas-Lehmer, que funciona muy bien con este tipo de números. Recordemos que un número de Mersenne es de la forma $2^n - 1$. Cuando dicho número es primo, se habla entonces de un «primo de Mersenne». Hasta el 10 de junio de 2009 sólo se conocían cuarenta y siete números primos de Mersenne. El más grande de ellos es $2^{43.112.609} - 1$, que tiene casi trece millones de cifras.

El proyecto Gimps

El Great Internet Mersenne Prime Search, la «Gran búsqueda de números primos de Mersenne por Internet», es un proyecto creado por George Woltman que consiste en una red colaboradora en la que los ordenadores personales de las personas que participan en el proyecto (cualquiera puede suscribirse) actúan en paralelo emulando capacidades muy superiores a las que pueda tener cualquier supercomputador actual. La idea es que cada usuario que quiere colaborar se instala el software adecuado, que le facilita la misma organización, y su ordenador trabaja en los tiempos muertos actuando como salvapantallas. El proyecto empezó a funcionar en 1997 y hasta agosto de 2009 se han encontrado un total de 12 números primos de

Mersenne. La Electronic Frontier Foundation (EFF), Fundación Frontera Electrónica, ofreció un premio de 150.000 dólares para el primero que descubriera un primo de Mersenne con un mínimo de diez millones de cifras. El premio fue adjudicado el 23 de agosto de 2008 a Edson Smith, del Departamento de Matemáticas de la UCLA, por el descubrimiento del número $2^{43.112.609} - 1$.



Logo de la Electronic Frontier Foundation.

5. ¿Cómo saber si un número es primo?

La única manera de saberlo con absoluta certeza es dividirlo por todos los números anteriores a él. Si no es divisible por ninguno de ellos, es primo. Sabemos, como hemos visto en un capítulo anterior, que podemos parar en la raíz cuadrada de dicho número. Para números pequeños y cálculos hechos a mano, es un buen método. Por ejemplo, vamos a averiguar si el número 101 es primo o compuesto. Para ello, el hecho de conocer los criterios de divisibilidad nos puede ahorrar algunos cálculos innecesarios. Ya sabemos que 101 no es divisible por 2, porque tendría que acabar en cero o en cifra par. Tampoco es divisible por 3, ya que la suma de sus cifras no es divisible por 3 ($1 + 0 + 1 = 2$). Asimismo, no es divisible por 5 porque tendría que acabar en 0 o en 5. También podemos saltarnos el 4, el 6 y el 9, ya que todos son múltiplos de 2 ó 3. Si probamos con el 7, nos da 14 de cociente y 3 de resto, luego tampoco es divisible por 7. El siguiente número que hay que probar es el 11 (evidentemente, 101 no es un múltiplo de 10). La división por 11 da de cociente 9 y de resto 2. Aquí ya podemos detenernos y afirmar que 101 es un número primo, ya que la raíz cuadrada de 101 es aproximadamente 10, lo que

nos garantiza con seguridad que no será divisible por ninguno de los números que quedan hasta 101.

Este método se conoce con el nombre de «división por tentativa», y es el más sencillo y seguro de todos. El problema es que no es viable para números muy grandes, ni siquiera mediante métodos informáticos. Pensemos que un número de cincuenta cifras requeriría calcular al menos hasta el orden de veinticinco cifras, que sería el que correspondería más o menos a su raíz cuadrada. En un ordenador con capacidad para realizar mil millones de divisiones por segundo necesitaríamos bastante más de trescientos millones de años para finalizar el cálculo, y para entonces lo más probable es que ya hubiera desaparecido la especie humana. De todas formas, hay que puntualizar que si se trata de un número compuesto y uno de sus factores no es excesivamente grande, el método puede funcionar. Hay que tener en cuenta que dado un número n cualquiera, la probabilidad de que el número 2 sea un factor de éste es del 50%; la de que 3 sea un factor, del 33%, y así sucesivamente.

Por otro lado, los ordenadores actuales han ido ganando en velocidad y capacidad de memoria lo suficiente como para que la búsqueda de un número primo en una larga lista resulte en algunos casos más eficaz que el complicado proceso de averiguar si un número dado es primo.

6. Pseudoprimos

El pequeño teorema de Fermat es uno de los más utilizados en los tests de primalidad. Recordemos que dicho teorema afirma lo siguiente: «Si p es primo no existe ninguna base a con $a < p$ (siendo a y p primos entre sí), de manera que $ap^{-1} - 1$ dé resto diferente de cero al dividirlo por p».

El teorema tiene sus limitaciones porque, como ya hemos visto, proporciona una condición necesaria pero no suficiente. Por ejemplo, si tomamos $p = 7$ tenemos que $3^6 - 1$ es divisible por 7.

Esto no nos garantiza que 7 sea un número primo (sabemos que lo es porque se trata de un número pequeño que hemos tomado para simplificar el ejemplo, pero debemos imaginar que estamos tratando con números grandes). En cambio, si tomamos $p = 8$ tendríamos que la división de $3^7 - 1$ da 273,25 y, por tanto, no es

divisible, lo que nos garantiza que 8 no es primo (sin necesidad de encontrar ninguno de sus factores).

El número que no pasa la prueba para una determinada base sabemos que es compuesto. A la base la llamamos entonces «testigo».

Si el número, en cambio, pasa la prueba y no es primo, llamamos al número de la base «mentiroso». Podemos entonces seguir haciendo pruebas. La probabilidad de encontrar mentirosos se va reduciendo en un factor 1/2 por cada prueba, con lo que la probabilidad de que el número sea primo va aumentando.

Un número *p* que, no siendo primo, pasa una prueba para una base a, se dice que es un «pseudoprimo» para dicha base. La definición más general de pseudoprimo es la siguiente: «Un número se dice que es pseudoprimo cuando pasa una prueba de número primo y resulta que es compuesto».

El asunto se complica cuando hay números que pasan las pruebas para cualquier base a y no son primos. Por ejemplo, el número 561 cumple con la prueba para cualquier base y es un número compuesto (561 = 3 · 11 · 17). A estos números, descubiertos por el matemático estadounidense Robert Daniel Carmichael (1879-1967), se los llama «números de Carmichael». Hasta ahora se conocen sólo 2.163 números de Carmichael, que se encuentran entre los primeros veinticinco mil millones de números naturales. Todos tienen al menos tres factores primos.

Hay dieciséis números de Carmichael menores de 100.000 y son: 561, 1.105, 1.729, 2.465, 2.821, 6.601, 8.911, 10.585, 15.841, 29.341, 41.041, 46.657, 52.633, 62.745, 63.973 y 75.361.

A los números de Carmichael se los llama también «pseudoprimos absolutos».

7. Los métodos

En la actualidad, los algoritmos que se utilizan para determinar si un número cualquiera es primo son de dos tipos: polinomial determinístico y polinomial probabilístico.

El primero garantiza de forma absoluta que se trata de un número primo, pero su tiempo de realización es alto. El segundo es más rápido, pero presenta una cierta aleatoriedad en el resultado.

El método más utilizado es el denominado «método de Miller-Rabin», una versión del test de primalidad de Fermat pero basado en la conjetura de Riemann. Es del tipo polinomial probabilístico, pero la probabilidad de que contenga un error se encuentra entre 1/1050 y 1/1080, por lo que en la práctica puede ser utilizado con garantías.

El 6 de agosto de 2002, tres investigadores del Instituto Tecnológico de Kanpur (India), M. Agrawal, N. Kayal y N. Saxena, publicaron un método determinístico en tiempo de ejecución polinomial basado en una generalización del pequeño teorema de Fermat:

$$n \text{ es primo} \Leftrightarrow (x-a)^n = x^n - a \text{ en el anillo } \frac{\mathbb{Z}_n[n]}{x'-1}$$

A pesar de ello, el método más usado sigue siendo el polinomial probabilístico dado su menor tiempo de realización.

La mayoría de los navegadores incluyen un algoritmo de encriptación que es capaz de encontrar por este tipo de métodos números primos grandes de hasta 2.048 bits, como los utilizados, por ejemplo, en las declaraciones de la renta o en el D.N.I.

Hoy día los tres sistemas utilizados en seguridad criptográfica son RSA, el logaritmo discreto en el grupo finito de un cuerpo finito (DSA) y el logaritmo discreto en una curva elíptica (ECDSA).

Ningún experto pone en duda la seguridad que proporciona cualquiera de estos tres sistemas. La diferencia entre ellos reside en la medida de las claves que se utilizan: la seguridad que otorgan las claves de 2.048 bits en los dos primeros es equivalente a utilizar claves de 224 bits en el tercero, con lo que el tiempo de cálculo se reduce considerablemente. Mientras que en los dos primeros se conocen algoritmos subexponenciales, en el tercero lo que hasta ahora se sabe utilizar mejor es de tipo exponencial.

Curiosidades numéricas

El número 313 es el de la matricula de los coches que suele utilizar el pato Donald. Tiene la curiosa propiedad de ser capicúa (puede leerse igual al

derecho que al revés), tanto en base 10 como en base 2, y es el único número primo de tres dígitos que posee esta propiedad: 313 (base 10) = 100111001 (base 2).

Y, además, 100111001 en base 10 es primo.

Existen muchos números primos que forman parte del elenco de curiosidades numéricas, como, por ejemplo, los llamados «repunit» (neologismo acuñado a partir de repeated unit), que están formados por largas series de unos, como 11111111111111111111111 (veintitrés unos), que es un número primo. En principio son sólo eso, curiosidades, aunque algún día estos números podrían llegar a formar parte de un teorema o conjetura de cierto valor matemático. Una serie curiosa de este tipo es la que se forma a partir del número 91, que es compuesto, 91 = 13 - 7, pero que cuando se le añade al final una serie de ceros terminados en 1, va alternado su carácter de primalidad:

9901 primo

999001 compuesto

99990001 primo

9999900001 compuesto

999999000001 primo

99999990000001 compuesto

9999999900000001 primo

999999999000000001 compuesto

Lamentablemente, el siguiente, 99999999990000000001, ya es un número compuesto.

8. Y la historia continúa...

Hemos visto que matemáticos como Mersenne, Fermat e incluso en ocasiones hasta el mismo Euler buscaban resultados prácticos. Muchas veces esto era en detrimento de una cierta consolidación teórica. Se eludían las demostraciones, pero seguían utilizándose los resultados.

Con Gauss se inició una nueva etapa de las matemáticas en donde el rigor de las demostraciones debía imperar sobre cualquier otro criterio. Pero en el caso de los

números primos parece que hemos retomado la vía empírica. Utilizamos teoremas no demostrados y damos por bueno un resultado confiando en que la probabilidad de cometer un error es muy baja. Hacemos como Fermat, pero sin necesidad de ocultar una hipotética demostración. A este escenario hemos llegado debido, por un lado, a la enorme capacidad de los algoritmos computacionales y, por otro, a la necesidad actual de disponer de grandes números primos.

En un nivel puramente teórico se puede afirmar que los números primos siguen resistiéndose a los matemáticos. Su historia es, en cierta medida, la historia de un fracaso. El máximo logro conseguido hay que buscarlo en la función zeta de Riemann, pero se tiene una clara conciencia de que éste es tan sólo un éxito parcial. Euler, que fue uno de los grandes visionarios de la matemática, no era especialmente optimista en cuanto a las posibilidades de éxito en la comprensión de estos esquivos números:

«Los matemáticos han intentado en vano desde hace mucho tiempo descubrir alguna secuencia en el orden de los números primos, pero tengo razones para creer que éste es un misterio en el que la mente humana jamás podrá penetrar».

Anexo
Demostraciones

1. Demostración del teorema fundamental de la aritmética

El teorema afirma que todo número natural diferente de 1 se puede expresar de forma única como producto de factores primos.

En primer lugar es preciso aclarar por qué se excluye a la unidad como número primo. Hay diversas razones, pero la más obvia es que de no ser así el teorema no se cumpliría, ya que el número 1, siendo primo, podría factorizarse de varias maneras: 1 = 1 x 1 = 1 x 1 x 1 = 1 x 1 x 1 x 1 = ...

Hecha esta salvedad, para demostrar el teorema se procede en dos pasos. En el primero se indica que existe la descomposición, y en el segundo, que ésta es única.

La primera parte se trabaja por reducción al absurdo. Supongamos que n es el número más pequeño que no puede ser descompuesto en factores primos. Sabemos que no puede ser 1 porque hemos descartado esta posibilidad en el mismo enunciado del teorema. Tampoco puede ser un número primo porque éste se descompone en sí mismo como tal; de modo que tiene que ser un número compuesto de la forma $n = a \times b$, con a y b menores que n. Pero como n era el menor que cumplía la condición de no poder descomponerse en factores primos, quiere decir que a y b sí lo hacen, por lo que forzosamente debe hacerlo también n, llegando de este modo a una contradicción.

La segunda parte de la demostración se basa en el siguiente resultado:

Si p es un número primo que divide un producto de factores, forzosamente tiene que dividir a alguno de esos factores. Este resultado puede demostrarse mediante la identidad de Bézout.

Supongamos que un número natural mayor que 1 se puede descomponer en factores primos de dos maneras diferentes: tomamos un número primo p de la primera descomposición. Necesariamente, dicho número debe dividir a la segunda descomposición y, por tanto, a alguno de sus factores.

Eligiendo el factor al que divide, como se trata de un factor primo, es necesario que sea igual a p. Ya hemos encontrado dos factores iguales en la descomposición.

Tomando ahora otro número primo seguiríamos el proceso hasta ver que los factores primos que figuran en ambas descomposiciones son todos iguales.

2. Demostración del pequeño teorema de Fermat

Expresado mediante congruencias, tal y como hemos visto en el capítulo 5, el teorema afirma que «Si *p* es un número primo, entonces para cada número natural a se tiene que $a^p \equiv a \ (mod\ p)$».

El teorema es equivalente a demostrar que *p* divide a $a^p - a$.

Demostraremos el teorema por el método de inducción sobre *a*, es decir, supondremos que es cierto para un número natural a y demostraremos entonces que también se cumple para *a* + 1.

De manera que partimos de la hipótesis de que *p* divide a $a^p - a$. Según el desarrollo del binomio de Newton, se tiene que:

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \ ... + \binom{p}{p-1} a + 1$$

Pasando al primer miembro los sumandos a^p y 1 nos queda:

$$(a+1)^p - a^p - 1 = \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \ ... + \binom{p}{p-1} a$$

El factor p está en todos los factoriales del segundo miembro, por lo que podemos afirmar que *p* divide al miembro de la derecha y, por tanto, también al de la izquierda, $(a + 1)^p - a^p - 1$.

Como, por hipótesis de inducción, *p* divide a $a^p - a$, podemos afirmar también que divide a la suma

$$[(a + 1)^p - a^p - 1] + a^p - a$$

Suma que, haciendo las operaciones convenientes, se puede expresar de la forma:

$$[(a + 1)^p - a^p - 1] + a^p - a = (a + 1)^p - (a + 1)$$

De este modo indicamos que también se cumple para a + 1 y, por tanto, queda demostrado el teorema.

Bibliografía

- Bentley, P. J., *El libro de las cifras*, Barcelona, Paidós, 2008.
- Durán, A. J., *Pasiones, piojos, dioses... y matemáticas*, Barcelona, Destino, 2009.
- Hardy, G. H., *Apología de un matemático*, Madrid, Nivola, 1995.
- Ifrah, G., *Las Cifras*, Madrid, Alianza, 1987.
- Kircher, P., *Aritmología*, Madrid, Breogán, 1984.
- Kline, M., *El pensamiento matemático*, Madrid, Alianza, 1994.
- Newman, J. R., *Srinivasa Ramanujan*, Barcelona, Blume, 1974.
- Pickover, C. A., *El prodigio de los números*, Barcelona, Ma non troppo, 2002.
- Sautoy, M. du, *La música de los números primos*, Barcelona, Acantilado, 2007.
- Stewart, I., *De aquí al infinito*, Madrid, Crítica (Grijalbo Mondadori), 1998.
  — *Historia de las matemáticas*, Madrid, Crítica, 2008.
- Szpiro, G., *La vida secreta de los números*, Córdoba, Almuzara, 2009.